GFI Product Manual

GFI LanGuard™

Administrator Guide

GFI®

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

All product and company names herein may be trademarks of their respective owners.

GFI LanGuard is copyright of GFI SOFTWARE Ltd. - 1999-2012 GFI Software Ltd. All rights reserved.

Document Version: 11.1

Last updated (month/day/year): 11/22/2012

Contents

1 Introduction **16**

1.1 How GFI LanGuard works 16
1.2 How GFI LanGuard Agents work 17
1.3 How GFI LanGuard Relay Agents work 17
1.4 GFI LanGuard Components 17
1.5 About this guide 18
1.5.1 Terms and conventions used in this manual 18

2 Installing GFI LanGuard **19**

2.1 Deployment scenarios 19
2.1.1 Deploying GFI LanGuard in mixed mode 19
2.1.2 Deploying GFI LanGuard using Relay Agents 20
2.1.3 Deploying GFI LanGuard in Agent-less mode 21
2.2 System requirements 23
2.2.1 Hardware requirements 23
2.2.2 Software requirements 24
2.2.3 Firewall Ports and Protocols 25
2.2.4 Gateway permissions 26
2.2.5 Supported antivirus/anti-spyware applications 27
2.3 Importing and Exporting Settings 27
2.3.1 Exporting configurations to a file 27
2.3.2 Importing configurations from a file 28
2.3.3 Importing configurations from another instance of GFI LanGuard 29
2.4 Upgrading from previous versions 30
2.5 New installation 32
2.6 Post install actions 35
2.7 Testing the installation 36

3 Achieving Results **38**

3.1 Effective Vulnerability Assessment 38
3.2 Effective Patch Management 39
3.3 Using GFI LanGuard for asset tracking 40
3.4 Up to date network and software analysis 41
3.5 Compliance with PCI DSS 42

4 Managing Agents **43**

4.1 Deploying Agents 43
4.2 Deploy Agents manually 45
4.3 Agent properties 47
4.4 Agents settings 52
4.5 Configuring Relay Agents 53
4.5.1 Configuring an Agent as a Relay 54
4.5.2 Configuring Relay Agent advanced options 58
4.5.3 Connecting computers to a Relay 60
4.6 Managing Agent groups 61

5 Scanning Your Network **64**
5.1 About Scanning Profiles 64
5.2 Available Scanning Profiles 64
5.2.1 Complete/Combination Scans 65
5.2.2 Vulnerability Assessment 65
5.2.3 Network & Software Audit 66
5.3 Manual scans 66
5.4 Enabling security audit policies 69
5.5 Scheduled scans 70
5.5.1 Creating a scheduled scan 71
5.5.2 Editing scheduled scan settings 79
5.5.3 Configuring scheduled scan properties 79
5.6 Agent scheduled scans 80
5.6.1 Starting an Agent scan manually 82

6 Dashboard **83**
6.1 Achieving results from the dashboard 83
6.2 Using the Dashboard 84
6.3 Using the Computer Tree 84
6.3.1 Simple filtering 85
6.3.2 Advanced filtering 85
6.3.3 Grouping 86
6.3.4 Searching 87
6.4 Using Attributes 88
6.4.1 Assigning attributes to a computer 88
6.4.2 Assigning attributes to a group 89
6.4.3 Configuring attributes 89
6.5 Dashboard actions 90
6.6 Exporting issue list 91
6.7 Dashboard views 91
6.7.1 Overview 92
6.7.2 Computers view 95
6.7.3 History view 97
6.7.4 Vulnerabilities View 98
6.7.5 Patches View 99
6.7.6 Ports View 100
6.7.7 Software View 101
6.7.8 Hardware View 102
6.7.9 System Information View 103

7 Interpreting Results **104**
7.1 Interpreting manual scan results 104
7.1.1 Viewing scan results 104
7.1.2 Vulnerability Level Rating 106
7.1.3 Vulnerability Assessment 108
7.1.4 Network & Software Audit 109
7.2 Loading results from the database 113

7.3 Saving and loading XML results 114

8 Remediate Vulnerabilities 116

8.1 Automatic Remediation 116
8.1.1 Auto-remediation notes 116
8.1.2 Configuring missing updates auto-deployment 117
8.1.3 Configuring unauthorized applications auto-uninstall 121
8.1.4 Configuring auto-remediation options 125
8.1.5 Configuring end-user reboot and shut down options 132
8.1.6 Configuring auto-remediation messages 132
8.1.7 Configuring Agent auto-remediation 136
8.2 Manual Remediation 138
8.2.1 Manual remediation notes 138
8.2.2 Using the Remediation Center 138
8.2.3 Deploying Software Updates 139
8.2.4 Uninstalling Software Updates 142
8.2.5 Deploying Custom Software 144
8.2.6 Uninstalling Custom Applications 145
8.2.7 Malware Protection 147
8.2.8 Using Remote Desktop Support 149

9 Activity Monitoring 151

9.1 Monitoring Security Scans 151
9.1.1 Filter Security Scans 152
9.2 Monitoring Software Updates Download 153
9.2.1 Troubleshooting failed Software Updates 154
9.3 Monitoring Remediation Operations 155
9.3.1 Remediation Jobs sub-tab 155
9.3.2 Remediation Operations view 157
9.4 Monitoring Product Updates 158

10 Reporting 159

10.1 Available reports 159
10.1.1 General reports 159
10.1.2 Legal Compliance reports 162
10.2 Generating reports 165
10.3 Scheduling Reports 167
10.3.1 Creating new scheduled reports 167
10.3.2 Configuring scheduled reports options 169
10.3.3 Managing scheduled reports 169
10.4 Customizing default reports 170
10.4.1 Creating custom reports 170
10.4.2 Customizing report logos 172
10.4.3 Customizing Email Report Format 173
10.5 Full text searching 174

11 Customizing GFI LanGuard 177

11.1 Configuring Alerting Options 177

11.2 Configuring Database Maintenance Options 178
11.2.1 Using Access™ as a database backend 178
11.2.2 Using SQL Server® as a database backend 179
11.2.3 Managing saved scan results 181
11.2.4 List scanned computers 182
11.2.5 Configure advanced database maintenance options 182
11.2.6 Configure database retention options 183
11.3 Configuring Program Updates 184
11.3.1 Configuring proxy settings 184
11.3.2 Configuring auto-update options 185
11.3.3 Installing program updates manually 186

12 Scanning Profile Editor 188

12.1 Create a new Scanning Profile 188
12.2 Configuring Vulnerabilities 189
12.2.1 Enabling vulnerability scanning 189
12.2.2 Customizing the list of vulnerabilities to be scanned 190
12.2.3 Customizing vulnerability checks properties 191
12.2.4 Setting up vulnerability check conditions 192
12.3 Configuring Patches 199
12.3.1 Enabling/disabling missing patch detection checks 200
12.3.2 Customizing the list of software patches to scan 200
12.3.3 Searching for Bulletin Information 201
12.4 Configuring Network & Software Audit options 202
12.4.1 Configuring TCP/UDP port scanning options 203
12.4.2 Configuring System Information options 204
12.4.3 Configuring Device scanning options 204
12.4.4 Configuring Applications scanning options 207
12.5 Configuring security scanning options 209

13 Utilities 212

13.1 DNS Lookup 212
13.2 Traceroute 215
13.3 Whois 216
13.4 Enumerate Computers 217
13.4.1 Starting a Security Scan 218
13.4.2 Deploying Custom Patches 218
13.4.3 Enabling Auditing Policies 218
13.5 Enumerate Users 219
13.6 SNMP Auditing 220
13.7 SNMP Walk 221
13.8 SQL Server® Audit 222
13.9 Command Line Tools 223
13.9.1 Using Insscmd.exe 223
13.9.2 Using deploycmd.exe 224
13.9.3 Using impex.exe 226

14 Script Debugger 228

14.1 Creating custom scripts using VBscript 228
14.1.1 Adding a vulnerability check that uses a custom VBScript (.vbs) 228
14.2 Creating custom scripts using Python Scripting 233
14.3 SSH Module 237
14.3.1 Keywords 237
14.3.2 Adding a vulnerability check that uses a custom shell script 238

15 Miscellaneous 243

15.1 Configuring NetBIOS 243
15.2 Uninstalling GFI LanGuard 244

16 Troubleshooting and support 245

16.1 Resolving common issues 245
16.2 Using the Troubleshooter Wizard 247
16.3 GFI SkyNet 249
16.4 Web Forum 249
16.5 Requesting technical support 249

17 Appendix 1 - Data Processed 251

17.1 System Patching Status 251
17.2 Ports 252
17.3 Hardware 252
17.4 Software 254
17.5 System Information 256

18 Appendix 2 - Certifications 259

18.1 Open Vulnerability and Assessment Language (OVAL) 259
18.1.1 GFI LanGuardOVAL Support 259
18.1.2 About OVAL Compatibility 260
18.1.3 Submitting OVAL listing error reports 260
18.2 Common Vulnerabilities and Exposures (CVE) 260
18.2.1 About CVE Compatibility 260
18.2.2 About CVE and CAN 261
18.2.3 Searching for CVE Entries 261
18.2.4 Obtaining CVE Names 261
18.2.5 Importing and Exporting CVE Data 261

19 Glossary 262

20 Index 270

List of Figures

Screenshot 1: Export configurations to file 28
Screenshot 2: Import configurations from a file 29
Screenshot 3: Import setting 30
Screenshot 4: Pre-requisite check dialog 31
Screenshot 5: Import and Export settings from a previous instance 32
Screenshot 6: End-user license agreement 33
Screenshot 7: Specify user details and license key 33
Screenshot 8: Attendant service credentials 34
Screenshot 9: Import and Export configurations 35
Screenshot 10: Launch a scan 36
Screenshot 11: Launch a scan properties 36
Screenshot 12: Scan results summary 37
Screenshot 13: Manage agents 44
Screenshot 14: Add more computers - Select import type 45
Screenshot 15: Add more computers - Assign attributes to new computers 46
Screenshot 16: Agent Properties - General tab 48
Screenshot 17: Agent Properties - Agent Status tab 49
Screenshot 18: Agent Properties - Attributes tab 50
Screenshot 19: Agent Properties - Relays tab 51
Screenshot 20: Agent Settings - General tab 52
Screenshot 21: Agent Settings - Advanced tab 53
Screenshot 22: Agent Properties dialog 55
Screenshot 23: Set computer as relay wizard 56
Screenshot 24: Choose caching directory for the new Relay Agent 57
Screenshot 25: Settings summary step 58
Screenshot 26: Relay Agent properties - Advanced settings 59
Screenshot 27: Relay Agent advances settings dialog 59
Screenshot 28: Connecting to a Relay Agent 61
Screenshot 29: Agent Attributes 62
Screenshot 30: Agent Relays 63
Screenshot 31: Manual scan settings 66
Screenshot 32: Custom target properties 67
Screenshot 33: Add new rule... 68
Screenshot 34: The audit policy administration wizard 70
Screenshot 35: New Scheduled Scan dialog 71
Screenshot 36: Scheduled scan frequency 72
Screenshot 37: Select scanning profile 73
Screenshot 38: Remote logon credentials 74

Screenshot 39: Scheduled scan reporting options 75
Screenshot 40: Scheduled scan auto-remediation options 76
Screenshot 41: Scheduled scan reporting options 77
Screenshot 42: Scheduled scan reporting options 78
Screenshot 43: Scheduled Scan properties 80
Screenshot 44: Agent Activity Recurrence 81
Screenshot 45: View Dashboard 84
Screenshot 46: Simple filtering 85
Screenshot 47: Add Filter Properties 86
Screenshot 48: Search specific computers and groups 87
Screenshot 49: Assigning attributes: Single computer 88
Screenshot 50: Assigning attributes: Multiple computers 89
Screenshot 51: New attribute dialog 90
Screenshot 52: Actions section in the Dashboard 90
Screenshot 53: Dashboard Overview 92
Screenshot 54: Analyze results by computer 95
Screenshot 55: History view in the Dashboard 97
Screenshot 56: Vulnerabilities view in the Dashboard 98
Screenshot 57: Patches view in Dashboard 99
Screenshot 58: Ports view in Dashboard 100
Screenshot 59: Software view in Dashboard 101
Screenshot 60: Hardware view in Dashboard 102
Screenshot 61: System Information view in Dashboard 103
Screenshot 62: Results overview 105
Screenshot 63: Vulnerability level meter 106
Screenshot 64: Dashboard Vulnerability Meter 107
Screenshot 65: The Vulnerability Assessment node 108
Screenshot 66: Bulletin info dialog 109
Screenshot 67: The network and software audit node 109
Screenshot 68: System patches status 110
Screenshot 69: All UDP and TCP ports, found during a scan 111
Screenshot 70: Reloaded scan results 114
Screenshot 71: Patch auto-deployment 118
Screenshot 72: Patch Auto-Deployment Advanced Options 119
Screenshot 73: Configuring Patch Auto-download Properties 120
Screenshot 74: Patch Repository settings 121
Screenshot 75: Unauthorized application 122
Screenshot 76: Applications inventory wizard 123
Screenshot 77: Application auto-uninstall validation 124
Screenshot 78: Computer properties 125

Screenshot 79: General auto-remediation settings 126
Screenshot 80: Before deployment options 127
Screenshot 81: After deployment options 128
Screenshot 82: Advanced deployment options 129
Screenshot 83: Device Manager 130
Screenshot 84: Power Management 131
Screenshot 85: Reboot/shut down options 132
Screenshot 86: Remediation Center - Deploy Software Updates 133
Screenshot 87: Deployment options dialog 134
Screenshot 88: Before Deployment Message options 135
Screenshot 89: Customizing warning messages 136
Screenshot 90: Agent auto-remediation 137
Screenshot 91: Remediation center 139
Screenshot 92: Deploying software updates 140
Screenshot 93: Deploy software updates options 141
Screenshot 94: Uninstalling software updates 142
Screenshot 95: Uninstall software updates options 143
Screenshot 96: List of software to be deployed 144
Screenshot 97: Uninstall applications 146
Screenshot 98: Malware protection 148
Screenshot 99: Remote desktop connection 149
Screenshot 100: Monitoring security scans 151
Screenshot 101: Filter security scan dialog 152
Screenshot 102: Security updates download 153
Screenshot 103: Monitoring jobs from the Remediation jobs sub-tab 156
Screenshot 104: Monitoring jobs from the Remediation Operations view 157
Screenshot 105: Product updates activity 158
Screenshot 106: Report sample - Part 1 165
Screenshot 107: Report sample - Part 2 166
Screenshot 108: Report sample - Part 3 166
Screenshot 109: Select scheduled report template 167
Screenshot 110: Add or remove target domains and/or computers 167
Screenshot 111: Edit scheduled reports options 170
Screenshot 112: Monitor scheduled reports activity 170
Screenshot 113: Edit report settings from the report sample preview 171
Screenshot 114: Configuring report items 171
Screenshot 115: Configuring report filtering options 172
Screenshot 116: Configure report grouping and sorting options 172
Screenshot 117: Customize the report parameters 175
Screenshot 118: Navigate using report links 176

Screenshot 119: Configuring Alerting Options 177
Screenshot 120: The database maintenance properties dialog 179
Screenshot 121: SQL Server® database backend options 180
Screenshot 122: Database maintenance properties: Managed saved scan results tab 181
Screenshot 123: Database Maintenance properties: Advanced tab 183
Screenshot 124: Configuring proxy server settings 185
Screenshot 125: Configure updates at application startup 186
Screenshot 126: Check for Updates wizard 187
Screenshot 127: The Scanning Profile Editor 189
Screenshot 128: Enabling vulnerability scanning for the selected scanning profile 190
Screenshot 129: Select the vulnerability checks to be run by this scanning profile 191
Screenshot 130: Vulnerability properties dialog: General tab 192
Screenshot 131: Vulnerability conditions setup tab 193
Screenshot 132: Check properties wizard - Select check type 194
Screenshot 133: Check properties wizard - Define the object to examine 195
Screenshot 134: Check properties wizard - Set required conditions 196
Screenshot 135: Check properties wizard - Defining conditional operators 197
Screenshot 136: Advanced vulnerability options 198
Screenshot 137: Advanced vulnerability scanning dialogs 199
Screenshot 138: Scanning Profiles properties: Patches tab options 200
Screenshot 139: Select the missing patches to enumerate 201
Screenshot 140: Searching for bulletin information 201
Screenshot 141: Extended bulletin information 202
Screenshot 142: Scanning Profiles properties: TCP Ports tab options 203
Screenshot 143: Scanning Profiles properties: System Information tab options 204
Screenshot 144: The network devices configuration page 205
Screenshot 145: The applications configuration page 207
Screenshot 146: Scanning Profiles properties: Scanner Options tab 210
Screenshot 147: DNS Lookup tool 213
Screenshot 148: DNS Lookup tool options 214
Screenshot 149: Traceroute tool 215
Screenshot 150: Whois tool 216
Screenshot 151: Enumerate Computers tool 217
Screenshot 152: The Enumerate Users tool dialog 219
Screenshot 153: SNMP Audit tool 220
Screenshot 154: SNMP Walk tool 221
Screenshot 155: SQL Server® Audit 222
Screenshot 156: Add vulnerability dialog 230
Screenshot 157: Adding vulnerability checks - Select type of check 231
Screenshot 158: Adding vulnerability checks - Select VB Script file 232

Screenshot 159: Adding vulnerability checks - Define conditions 233
Screenshot 160: Add vulnerability dialog 234
Screenshot 161: Adding vulnerability checks - Select type of check 235
Screenshot 162: Adding vulnerability checks - Select Python Script file 236
Screenshot 163: Adding vulnerability checks - Defining conditions 237
Screenshot 164: Add vulnerability dialog 239
Screenshot 165: Adding vulnerability checks - Select type of check 240
Screenshot 166: Adding vulnerability checks - Select SSH file 241
Screenshot 167: Adding vulnerability checks - Define conditions 242
Screenshot 168: Local Areas Connection properties: WINS tab 244
Screenshot 169: Troubleshooter wizard – Information details 248
Screenshot 170: Troubleshooter wizard – Gathering information about known issues 249
Screenshot 171: Searching for CVE information 261

List of Tables

Table 1: GFI LanGuard Components 18
Table 2: Terms and conventions used in this manual 18
Table 3: Hardware requirements - GFI LanGuard Server 23
Table 4: Hardware requirements - GFI LanGuard Agent 23
Table 5: Hardware requirements - GFI LanGuard Relay Agent 24
Table 6: Supported Operating Systems 24
Table 7: Software requirements - Additional components 25
Table 8: Ports and Protocols 26
Table 9: Override options 30
Table 10: Import override options 36
Table 11: Target selection 44
Table 12: Custom rules options 44
Table 13: Deploy Agents: Advanced Settings 45
Table 14: Add more computers wizard 45
Table 15: Attributes settings 46
Table 16: Agent relay options 51
Table 17: Relay agent advanced settings 51
Table 18: Agents settings 52
Table 19: Relay Agent - Advanced options 60
Table 20: Agent group status 61
Table 21: Agent group network discovery 62
Table 22: Agent relay options 63
Table 23: Complete/Combination scanning profiles 65
Table 24: Vulnerability assessment scanning profiles 65
Table 25: Network & Software Audit 66
Table 26: Target options when auditing 67
Table 27: Custom target properties 68
Table 28: Logon and audit options 69
Table 29: Scan options 69
Table 30: New scheduled scan type 71
Table 31: Remote logon credentials 74
Table 32: Power saving options 75
Table 33: Auto-remediation options 76
Table 34: Reporting options 77
Table 35: Options to manage scanning profiles 79
Table 36: Schedule scan properties 80
Table 37: Search options 87
Table 38: Dashboard actions 90

Table 39: Software information from an audit 92
Table 40: View by computers information 95
Table 41: Response time icons 105
Table 42: Vulnerability level weight scores 106
Table 43: Vulnerability groups 108
Table 44: Hardware information from an audit 111
Table 45: Software information from an audit 112
Table 46: System information from an audit 112
Table 47: Automatic remediation stages 117
Table 48: Patch Auto-Deployment Advanced Options 119
Table 49: Manage applicable schedule scans 124
Table 50: Before deployment 127
Table 51: After deployment 128
Table 52: Advanced deployment options 129
Table 53: Advanced deployment options 132
Table 54: Warning messages 136
Table 55: Remediation actions 139
Table 56: Deploy software updates options 141
Table 57: Uninstall software updates options 143
Table 58: Options available in Deploy Custom Software 144
Table 59: Deployment options 145
Table 60: Uninstall applications 146
Table 61: Deployment options 148
Table 62: Filter security scan dialog 152
Table 63: Updates download status 153
Table 64: Security updates download 154
Table 65: Troubleshooting failed Software Updates 154
Table 66: Available General Reports 160
Table 67: Available Legal Compliance Reports 162
Table 68: Scheduled report template options 167
Table 69: Target Domains & Computers options 167
Table 70: Scheduling options 168
Table 71: Alerting & Saving Settings 169
Table 72: Report placeholders 173
Table 73: Mail settings parameters 178
Table 74: Notifications options 178
Table 75: Database retention options 184
Table 76: Proxy settings 185
Table 77: Vulnerability properties dialog 192
Table 78: TCP Port scanning options 203

Table 79: Device scanning options 206
Table 80: Applications scanning options 207
Table 81: Scanner Options 210
Table 82: DNS lookup options 213
Table 83: Traceroute icons 215
Table 84: Enumerate computers options 217
Table 85: Insscmd command switches 223
Table 86: Supported variables in lnssmcd 224
Table 87: deploycmd command switches 225
Table 88: impex command switches 226
Table 89: Vulnerability keywords 238
Table 90: GFI LanGuard common Issues 245
Table 91: Information gathering options 248
Table 92: CVE Compatibility 260

1 Introduction

GFI LanGuard is a patch management and network auditing solution that enables you to easily manage and maintain end-point protection across devices within your LAN. It acts as a virtual security consultant that offers Patch Management, Vulnerability Assessment and Network Auditing support for Windows®and MAC computers. GFI LanGuard achieves LAN protection through:

- Identification of system and network weaknesses via a comprehensive vulnerability checks data-base. This includes tests based on OVAL, CVE and SANS Top 20 vulnerability assessment guidelines
- Auditing of all hardware and software assets on your network, enabling you to create a detailed inventory of assets. This goes as far as enumerating installed applications as well as devices connected on your network
- Automatic download and remote installation of service packs and patches for Microsoft® Windows and MAC operating systems as well as third party products
- Automatic un-installation of unauthorized software.

Topics in this chapter:

1.1 How GFI LanGuard works 16

1.2 How GFI LanGuard Agents work 17

1.3 How GFI LanGuard Relay Agents work 17

1.4 GFI LanGuard Components 17

1.5 About this guide 18

1.1 How GFI LanGuard works

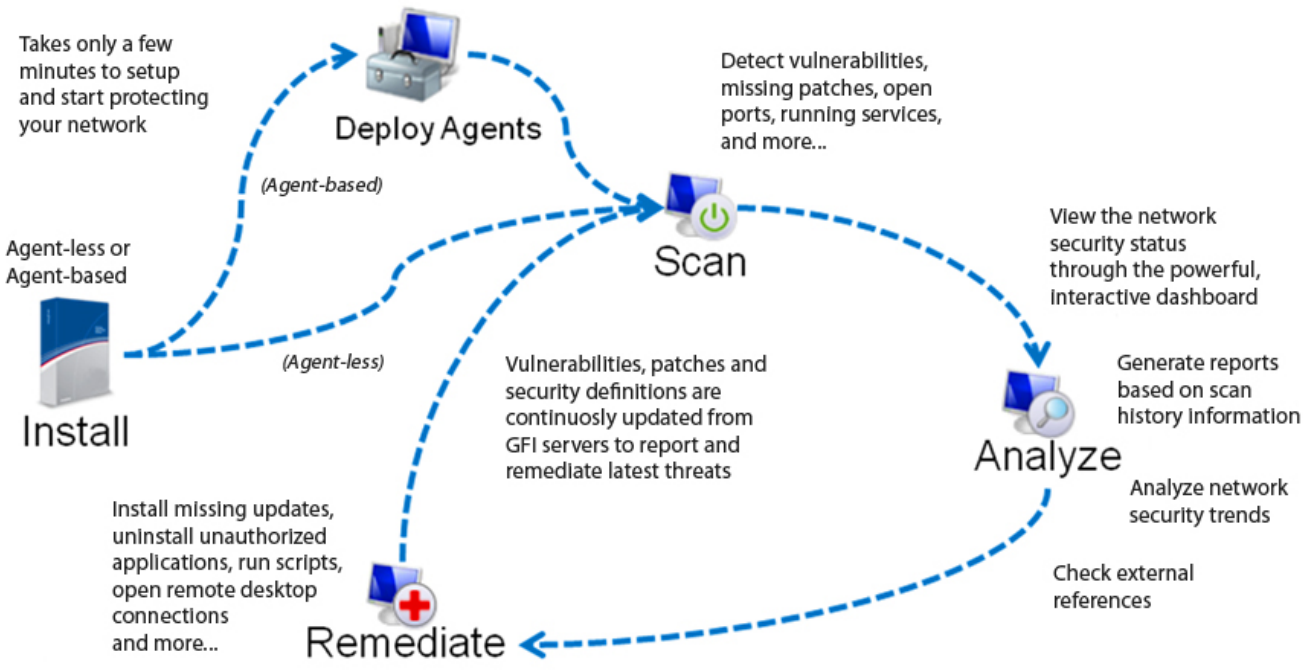

Takes only a few minutes to setup and start protecting your network
Deploy Agents
(Agent-based)
Detect vulnerabilities, missing patches, open ports, running services, and more...
Agent-less or Agent-based
Scan
View the network security status through the powerful, interactive dashboard
Install
(Agent-less)
Vulnerabilities, patches and security definitions are continuosly updated from GFI servers to report and remediate latest threats
Generate reports based on scan history information
Analyze
Analyze network security trends
Install missing updates, uninstall unauthorized applications, run scripts, open remote desktop connections and more...
Check external references
Remediate

Figure 1: How GFI LanGuard works

Upon installation, GFI LanGuard operates in two stages:

- First it determines the machines that are reachable. It also tries to collect information sets from the target machines as part of its Network Discovery operations, using a subset of SMB, NETBIOS, and ICMP protocols. Supported targets include the localhost, IP, computer name, computers list, IP range, whole domain/workgroup and/or organizational unit.
- Second, once the targets are identified, GFI LanGuard performs a deep scan to enumerate all the information related to the target computer. GFI LanGuard uses a variety of techniques to gain access to this information ranging from file and folder property checks, registry checks, WMI commands, SMB commands as well as port scan checks (TCP/UDP) and more.

1.2 How GFI LanGuard Agents work

GFI LanGuard can be configured to automatically discover and deploy agents on new computers. Agents minimize network bandwidth utilization. This is because in Agent-less mode, the GFI LanGuard server component performs audits over the network; while in Agent mode, audits are done using the scan target's resources and only a result XML file is transferred over the network.

Agents send scan data to GFI LanGuard through TCP port 1070. This port is opened by default when installing GFI LanGuard. Agents do not consume resources of the scan target's machine unless it is performing a scan or remediation operations. If an Agent becomes unresponsive for 60 days, it is automatically uninstalled from the target machine.

Note

By default, Agents auto-uninstall after 60 days. To customize the timeframe, go to **Configuration** tab > **Agents Management** and from the right pane, click **Agents Settings**. Specify the number of days in the **General** tab of the **Agents Settings** dialog.

Note

Agents can only be installed on computers running a Microsoft Windows operating system and they require approximately 25 MB of memory and 350 MB of hard disc space.

1.3 How GFI LanGuard Relay Agents work

GFI LanGuard enables you to configure any machine with a GFI LanGuard Agent installed on it, to act as a GFI LanGuard server. These Agents are called **Relay Agents**. Relay Agents reduce the load from the GFI LanGuard server component. Computers configured as relay agents download patches and definitions directly from the GFI LanGuard server and forward them to client computers just as if it were the server component.

1.4 GFI LanGuard Components

This section provides you with information about components that are installed by default, when you install GFI LanGuard. Once you install the product, you can manage patch management and remediation tasks from the Management Console. The Management Console is also referred to as the Server component of GFI LanGuard, as described in the table below:

Table 1: GFI LanGuard Components

Component	Description
GFI LanGuard Server	Also knows as the Management Console. Enables you to manage agents, perform scans, analyze results, remediate vulnerability issues and generate reports.
GFI LanGuard Agents	Enable data processing and auditing on target machines; once an audit is finished, result is sent to GFI LanGuard.
GFI LanGuard Update System	Enables you to configure GFI LanGuard to auto-download updates released by GFI to improve functionality. These updates also include checking GFI web site for newer builds.
GFI LanGuard Attendant Service	The background service that manages all scheduled operations, including scheduled network security scans, patch deployment and remediation operations.
GFI LanGuard Scanning Profiles Editor	This editor enables you to create new and modify existing scanning profiles.
GFI LanGuard Command Line Tools	Enables you to launch network vulnerability scans and patch deployment sessions as well as importing and exporting profiles and vulnerabilities without loading up the GFI LanGuard management console.

1.5 About this guide

The aim of this Administrator Guide is to help System Administrators install, configure and run GFI LanGuard with minimum effort.

1.5.1 Terms and conventions used in this manual

Table 2: Terms and conventions used in this manual

Term	Description
	Additional information and references essential for the operation of GFI LanGuard.
	Important notifications and cautions regarding potential issues that are commonly encountered.
>	Step by step navigational instructions to access a specific function.
Bold text	Items to select such as nodes, menu options or command buttons.
Italics text	Parameters and values that you must replace with the applicable value, such as custom paths and file names.
`Code`	Indicates text values to key in, such as commands and addresses.

2 Installing GFI LanGuard

This chapter guides you in selecting the most appropriate deployment solution that caters to your requirements as well as provides you with information about how to successfully deploy a fully functional instance of GFI LanGuard.

Topics in this chapter:

2.1 Deployment scenarios 19

2.2 System requirements 23

2.3 Importing and Exporting Settings 27

2.4 Upgrading from previous versions 30

2.5 New installation 32

2.6 Post install actions 35

2.7 Testing the installation 36

2.1 Deployment scenarios

GFI LanGuard can be installed on any machine which meets the minimum system requirements. Use the information in this section to determine whether you want to monitor a pool of Agent-less, Agent-based or a mix of both, depending on the:

- Number of computers and devices you want to monitor
- Traffic load on your network during normal operation time.

The following sections provide you with information about different deployment scenarios supported by GFI LanGuard:

- Deploying GFI LanGuard in mixed mode
- Deploying GFI LanGuard using Relay Agents
- Deploying GFI LanGuard in Agent-less mode

2.1.1 Deploying GFI LanGuard in mixed mode

GFI LanGuard can be configured to deploy agents automatically on newly discovered machines or on manually selected computers. Agents enable data processing and auditing to be done on target machines; once an audit is finished, the result is transferred to GFI LanGuard through an XML file. Agent-based scans:

- Have better performance because the load is distributed across client machines.
- Can work on low bandwidth environments because the communication between the server and agents is reduced.
- Are suitable for laptops. Computers will be scanned even if the computer is not connected to the company network.
- Are more accurate than manual scans, agents can access more information on the local host.

The following screenshot shows how GFI LanGuard can be deployed using agents on a Local Area Network (LAN):

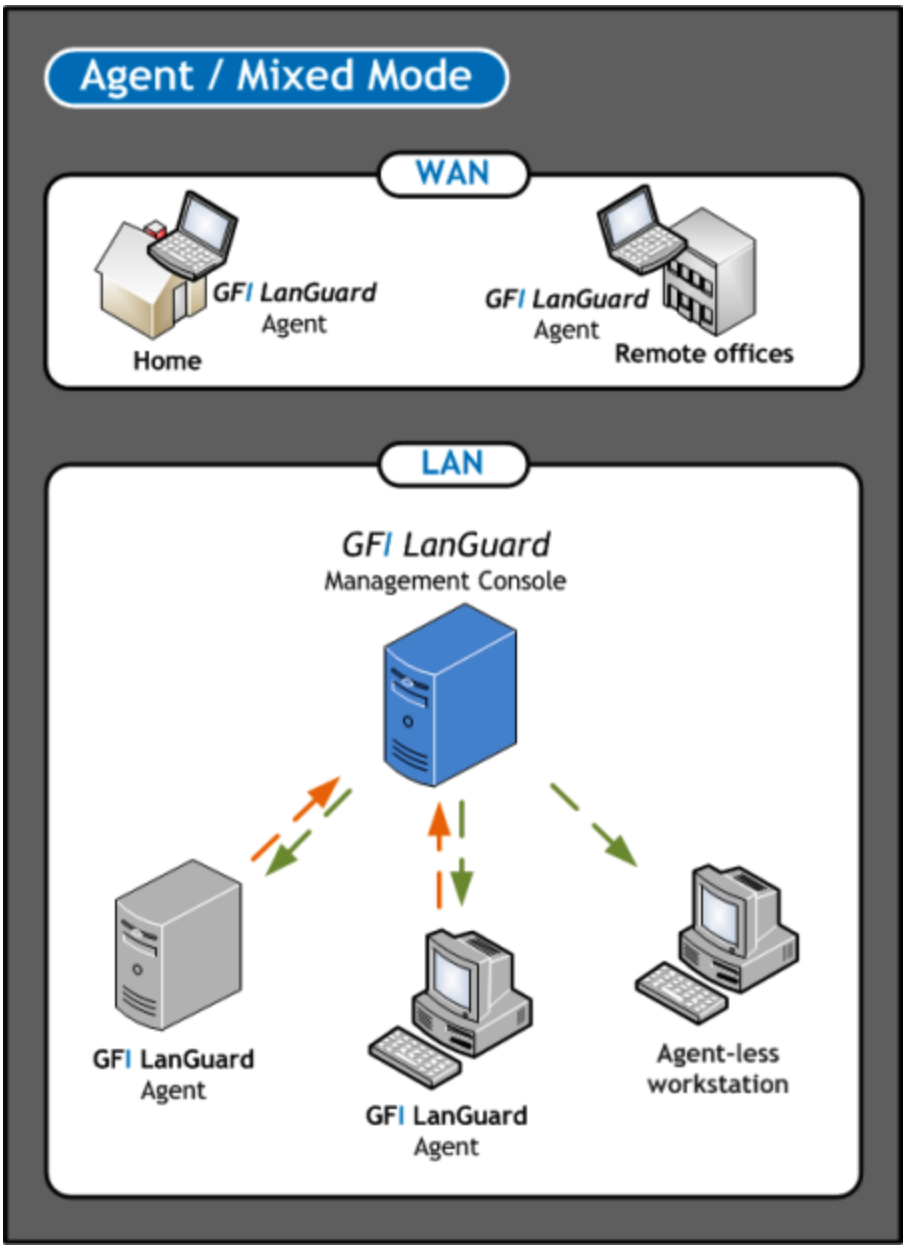


Figure 2: Agent/Mixed Mode

2.1.2 Deploying GFI LanGuard using Relay Agents

Relay agents are used to reduce the load from the GFI LanGuard server. Computers configured as relay agents will download patches and definitions directly from the GFI LanGuard server and will forward them to client computers. The main advantages of using relay agents are:

- Save Network Bandwidth in local or geographically distributed networks. If a relay agent is configured on each site, a patch is only downloaded once and distributed to clients
- Load is removed from the GFI LanGuard server component and distributed amongst relay agents
- Since computers are managed from multiple relay agents, it increases the number of devices that can be protected simultaneously.

In a network, computers can be grouped and each group can be assigned to a relay agent as shown below.

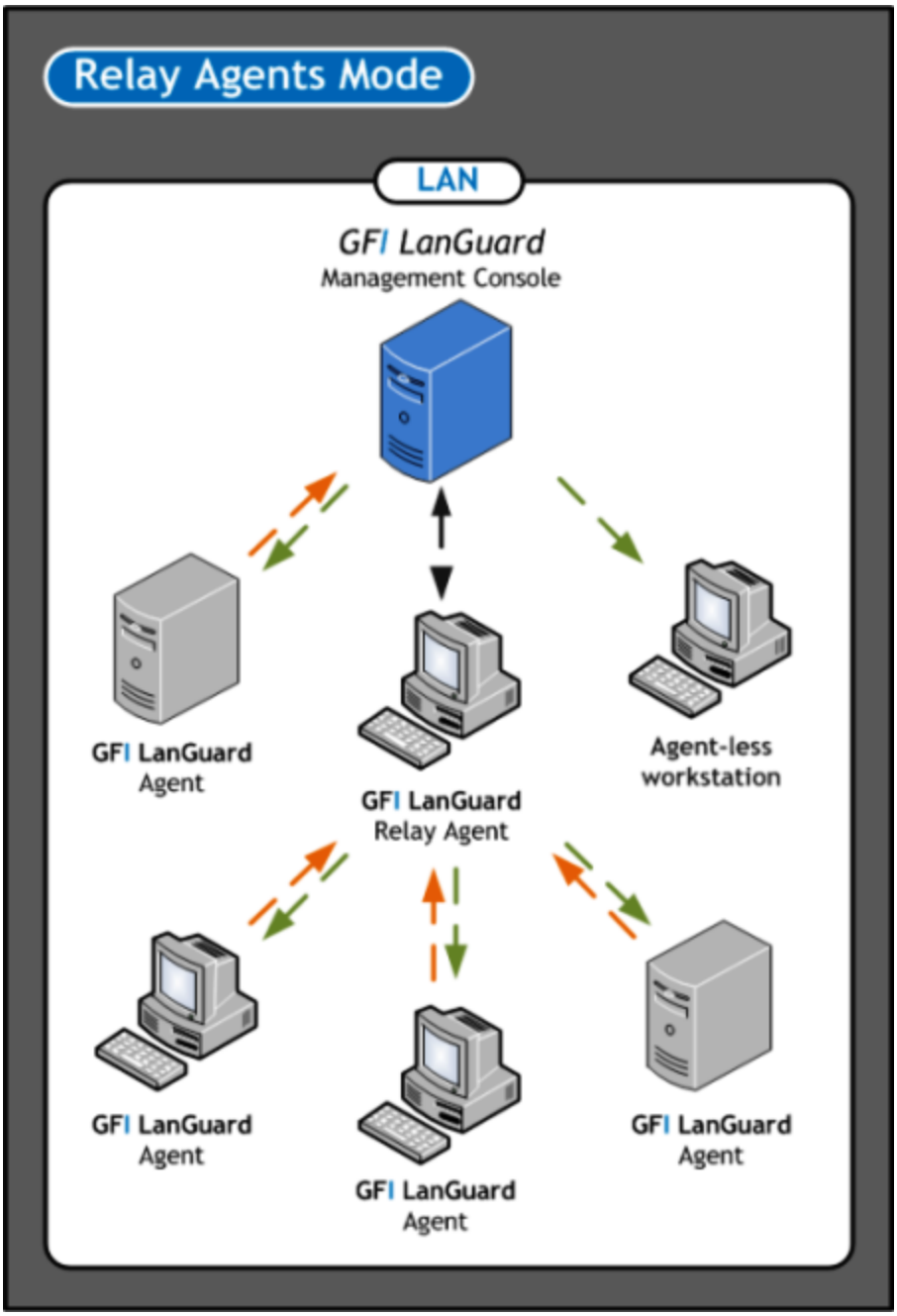


Figure 3: Relay Agent Mode

Note

For more information, refer to Configuring Relay Agents (page 53).

2.1.3 Deploying GFI LanGuard in Agent-less mode

Agent-less auditing is started from the GFI LanGuard management console. GFI LanGuard creates a remote session with the specified scan targets and audits them over the network. On completion, the results are imported into the results database and the remote session ends.

You can audit single computers, a range of specific computers and an entire domain/workgroup.

Note

Scans in Agent-less mode use the resources of the machine where GFI LanGuard is installed and utilize more network bandwidth since auditing is done remotely. When you have a large network of scan targets, this mode can drastically decrease GFI LanGuard's performance and affects network speed. In larger networks, deploy Agents/Relay Agents to balance the load appropriately.

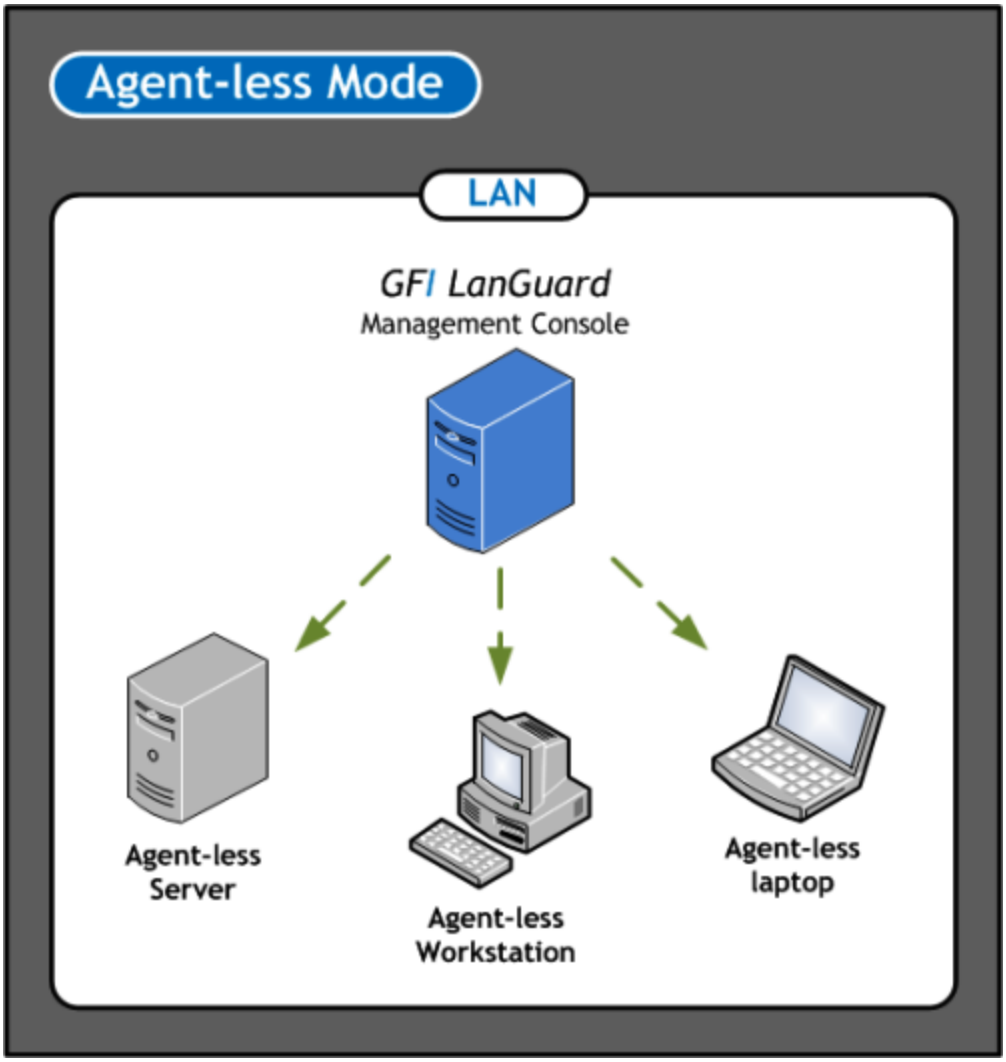


Figure 4: Agent-Less Mode

2.2 System requirements

Computers that are going to run GFI LanGuard Server/Agent/Relay Agent must meet the system requirements described below to ensure maximum and optimized performance. If you are looking for a patch management solution for 2,000 or more computers, we recommend that you contact us for pricing, as well as suggestions regarding the proper deployment and management procedure for such a solution. Refer to the following sections for information about:

- Hardware requirements
- Software requirements
- Firewall ports and protocols
- Gateway permissions
- Supported antivirus/anti-spyware applications

2.2.1 Hardware requirements

Ensure that the hardware requirements specified below are met, on computers running any of the following components:

- GFI LanGuard Server
- GFI LanGuard Agent
- GFI LanGuard Relay Agent

GFI LanGuard Server

Computers hosting GFI LanGuard Server must meet the following hardware requirements:

Table 3: Hardware requirements - GFI LanGuard Server

Component	1 to 100 Computers	100 to 500 Computers	500 to 3,000 Computers
Processor	2 GHz Dual Core	2.8 GHz Dual Core	3 GHz Quad Core
Physical Storage	5 GB	10 GB	20 GB
RAM	2 GB	4 GB	8 GB
Network bandwidth	1544 kbps	1544 kbps	1544 kbps

GFI LanGuard Agent

Computers running a GFI LanGuard Agent must meet the following hardware requirements:

Table 4: Hardware requirements - GFI LanGuard Agent

Component	Requirement
Processor	1 GHz
Physical Storage	350 MB
RAM	25 MB
Network bandwidth	1544 kbps

GFI LanGuard Relay Agent

A computer is eligible to be configured as a Relay Agent when:

- The computer is online and has good uptime
- Has fast network access to computers connected to it

- Has the required disk space to allow caching.

Computers configured as Relay Agents must meet the following hardware requirements:

Table 5: Hardware requirements - GFI LanGuard Relay Agent

Component	1 to 100 Clients	100 to 500 Clients	500 to 1,000 Clients
Processor	2 GHz Dual Core	2 GHz Dual Core	2.8 GHz Dual Core
Physical Storage	5 GB	10 GB	10 GB
RAM	2 GB	2 GB	4 GB
Network bandwidth	100 Mbps	100 Mbps	1 Gbps

2.2.2 Software requirements

GFI LanGuard components can be installed on any computer that meets the software requirements listed in this section. For more information, refer to:

- Supported operating systems
- Supported database backends
- Target computer components
- Other software components

Supported operating systems (32-bit/64-bit)

The following table lists operating systems that GFI LanGuard Server/Agent/Relay Agent can be installed on:

Table 6: Supported Operating Systems

Operating System	GFI LanGuard	GFI LanGuard Agent	GFI LanGuard Relay Agent
Windows ® Server 2012	✓	✓	✓
Windows® Server 2008 (including R2) Standard/Enterprise	✓	✓	✓
Windows® Server 2003 Standard/Enterprise	✓	✓	✓
Windows® 8	✓	✓	✓
Windows® 7 Professional/Enterprise/Ultimate	✓	✓	✓
Windows® Vista Business/Enterprise/Ultimate	✓	✓	✓
Windows® XP Professional (SP2 or higher)	✓	✓	✓
Windows® Small Business Server 2008 Standard	✓	✓	✓
Windows® Small Business Server 2003 (SP1)	✓	✓	✓
Windows® 2000 Professional/Server/Advanced » SP4 » Internet Explorer 6 SP1 or higher » Windows Installer 3.1 or higher	✗	✓	✓

Supported database backends

The database backend is the location where GFI LanGuard stores scan and network information from network security audits and remediation operations. The database backend can be any of the following:

- Microsoft® Access
- SQL Server® 2000 or later
- MSDE/SQL Server Express® edition.

Target computer components

The following table provides you with information about components that are required to be installed/enabled on computers to be scanned remotely by GFI LanGuard:

Table 7: Software requirements - Additional components

Component	Description
Secure Shell (SSH)	Required for UNIX based scan targets. Commonly included as part of all major Unix/Linux distributions.
Windows Management Instrumentation (WMI)	Required to scan Windows-based scan targets. Included in all Windows 2000 or newer operating systems.
File and Printer Sharing	Required to enumerate and collect information about scan targets.
Remote Registry	Required for GFI LanGuard to run a temporary service for scanning a remote target.

Additional GFI LanGuard Server components

The following additional component is required on the computer where the GFI LanGuard Server component is installed:

- Microsoft .NET® Framework 3.5.

2.2.3 Firewall Ports and Protocols

This section provides you with information about the required firewall ports and protocols settings for:

- GFI LanGuard Server and Relay Agents
- GFI LanGuard Agent and Agent-less computers

GFI LanGuard and Relay Agents

Configure your firewall to allow **Inbound** connections on TCP port **1070**, on computers running:

- GFI LanGuard
- Relay Agents

This port is automatically used when GFI LanGuard is installed, and handles all inbound communication between the server component and the monitored computers. If GFI LanGuard detects that port 1070 is already in use by another application, it automatically searches for an available port in the range of **1070-1170**.

To manually configure the communication port:

1. Launch GFI LanGuard.

2. Click **Configuration** tab **> Manage Agents**.

3. From the right pane, click **Agents Settings**.

4. From the **Agents Settings** dialog, specify the communication port in the **TCP port** text box.

5. Click **OK**.

GFI LanGuard Agent and Agent-less computers

GFI LanGuard communicates with managed computers (Agents and Agent-less), using the ports and protocols below. The firewall on managed computers needs to be configured to allow **Inbound** requests on ports:

Table 8: Ports and Protocols

TCP Ports	Protocol	Description
22	SSH	Auditing Linux systems.
135	DCOM	Dynamically assigned port.
137	NetBIOS	Computer discovery and resource sharing.
138	NetBIOS	Computer discovery and resource sharing.
139	NetBIOS	Computer discovery and resource sharing.
161	SNMP	Computer discovery.
445	SMB	Used while: » Auditing computers » Agent management » Patch deployment.

2.2.4 Gateway permissions

To download definition and security updates, GFI LanGuard connects to GFI, Microsoft and Third-Party update servers via HTTP. Ensure that the firewall settings of the machine where GFI LanGuard is installed, allows connections to:

- *software.gfi.com/lnsupdate/
- *.download.microsoft.com
- *.windowsupdate.com
- *.update.microsoft.com
- All update servers of Third-Party Vendors supported by GFI LanGuard.

Note

For more information, refer to:

- Supported Third-Party applications:
  - http://go.gfi.com/?pageid=LAN_PatchMng
- Supported application bulletins:
  - http://go.gfi.com/?pageid=3p_fullreport
- Supported Microsoft applications:
  - http://go.gfi.com/?pageid=ms_app_fullreport
- Supported Microsoft bulletin:
  - http://go.gfi.com/?pageid-ms_fullreport

2.2.5 Supported antivirus/anti-spyware applications

GFI LanGuard, detects outdated definition files for a number of Anti-virus and Anti-spyware software. For a full list of supported Anti-virus and Anti-spyware software, refer to: http://go.gfi.com/?pageid=security_app_fullreport

2.3 Importing and Exporting Settings

GFI LanGuard enables you to import and export settings. Settings that can be Imported/Exported include:

- Scanning Profiles
- Vulnerability Assessment
- Ports (TCP/UDP)
- Results Filtering Reports
- Auto-Remediate Settings (Auto-Uninstall and Patch settings)
- Options (Database Backend, Alerting, Schedule scan and Internal Settings).

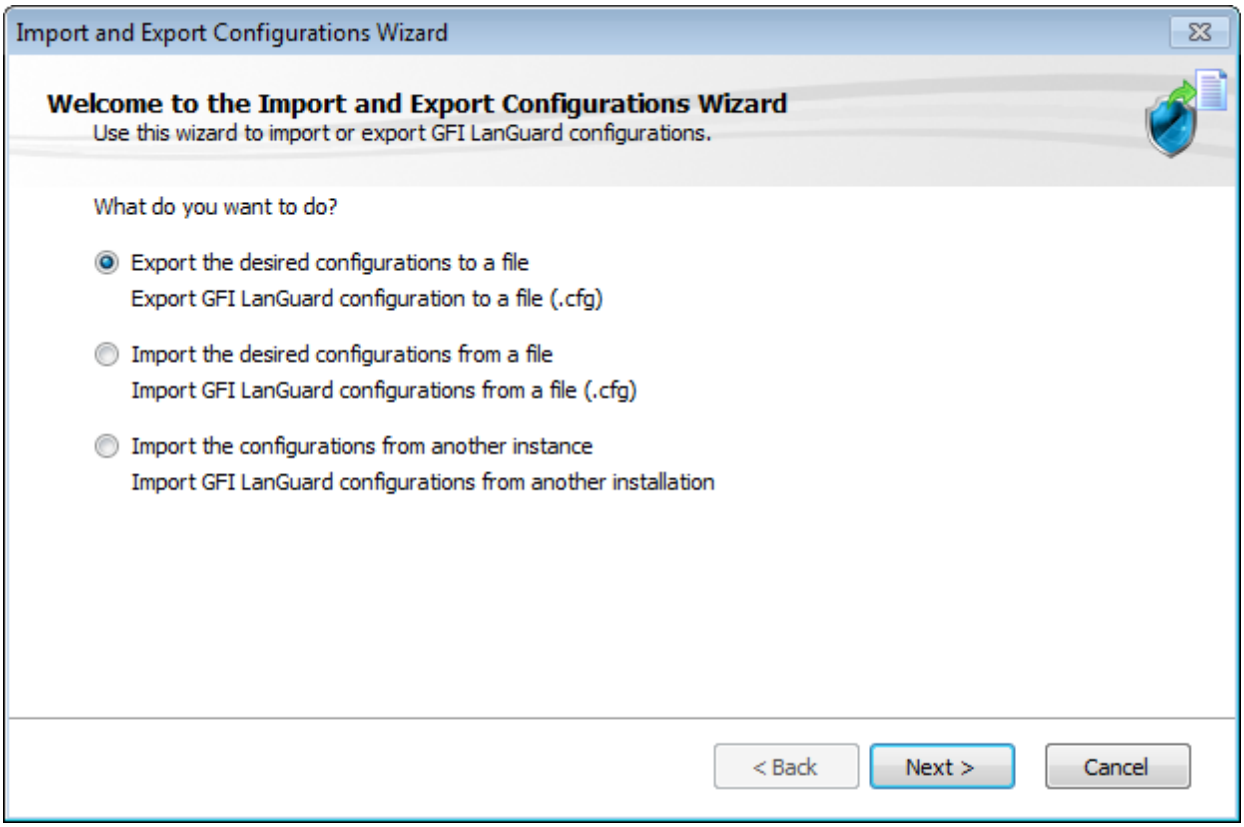
The following sections contain information about:

- Exporting configurations to a file
- Importing configurations from a file
- Importing configurations from another instance of GFI LanGuard

2.3.1 Exporting configurations to a file

To export the configurations:

1. Launch GFI LanGuard.
2. Click the **GFI LanGuard button > File > Import and Export Configurations...**
3. Select **Export the desired configuration to a file** and click **Next**.
4. Specify the path were to save the exported configuration, and click **Next**.


Import and Export Configurations Wizard
Welcome to the Import and Export Configurations Wizard
Use this wizard to import or export GFI LanGuard configurations.
What do you want to do?
Export the desired configurations to a file
Export GFI LanGuard configuration to a file (.cfg)
Import the desired configurations from a file
Import GFI LanGuard configurations from a file (.cfg)
Import the configurations from another instance
Import GFI LanGuard configurations from another installation
< Back
Next >
Cancel

Screenshot 1: Export configurations to file

5. Wait for the configuration tree to load and select the configurations to export. Click **Next** to start export.

6. A notify dialog will confirm that exporting is completed.

7. Click **OK** to finish.

2.3.2 Importing configurations from a file

To import saves configurations:

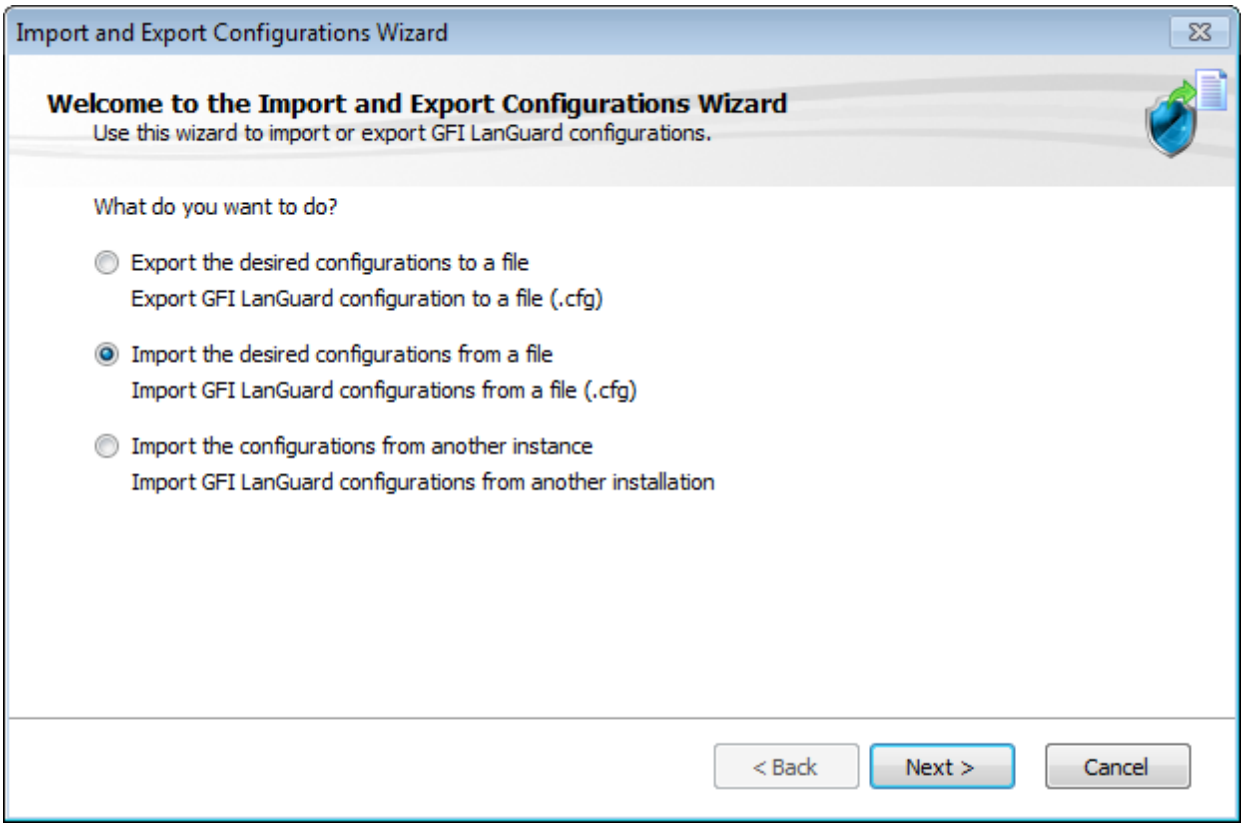
1. Launch GFI LanGuard.

2. Click the **GFI LanGuard button > File > Import and Export Configurations…**

3. Select Import the desired configuration from a file and click **Next**.

4. Specify the path from where to load configuration, and click **Next**.

5. Wait for the configuration tree to load and select the configurations to import. Click **Next** to start import.


Import and Export Configurations Wizard
Welcome to the Import and Export Configurations Wizard
Use this wizard to import or export GFI LanGuard configurations.
What do you want to do?
Export the desired configurations to a file
Export GFI LanGuard configuration to a file (.cfg)
Import the desired configurations from a file
Import GFI LanGuard configurations from a file (.cfg)
Import the configurations from another instance
Import GFI LanGuard configurations from another installation
< Back
Next >
Cancel

Screenshot 2: Import configurations from a file

6. Confirm the override dialog box; by clicking, **Yes** or **No** as required.

7. A notify dialog will confirm that exporting is completed

8. Click **OK** to finish.

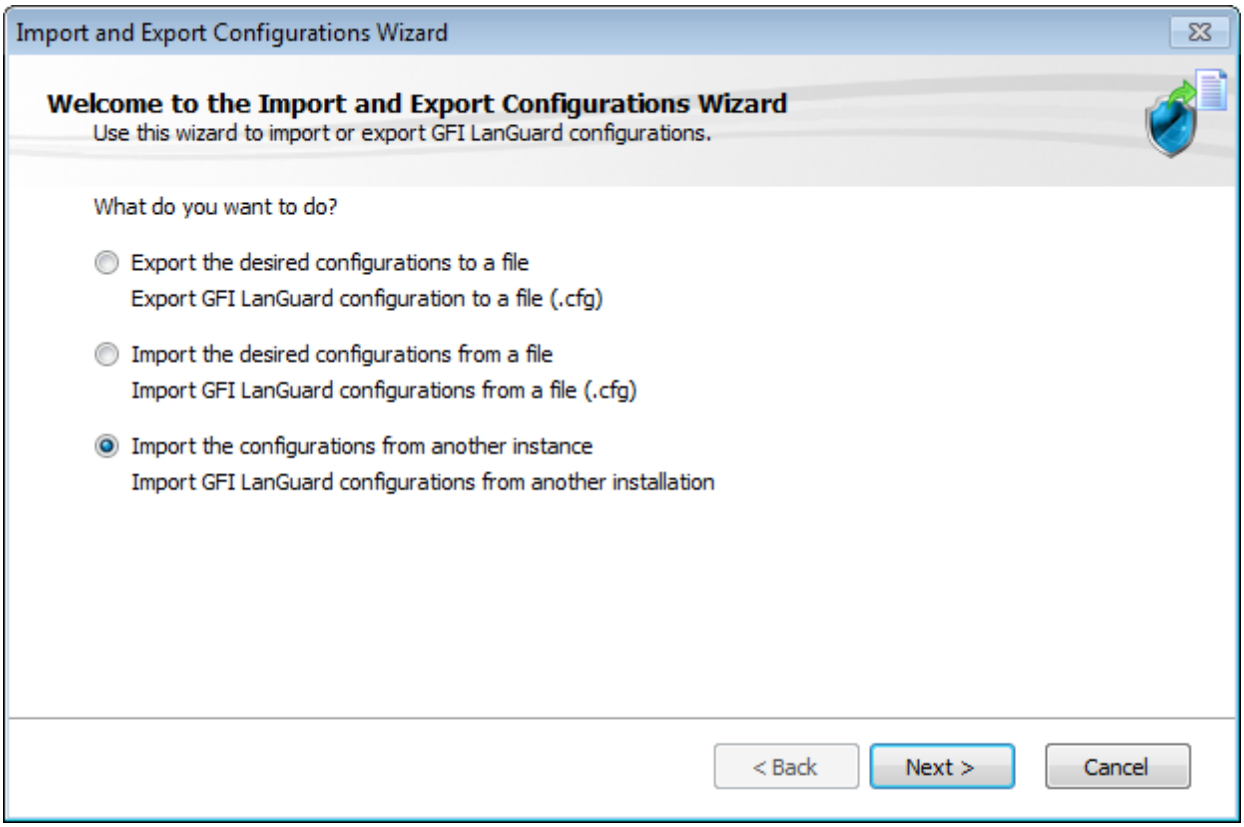
2.3.3 Importing configurations from another instance of GFI LanGuard

1. Launch GFI LanGuard.

2. Click the **GFI LanGuard button > File > Import and Export Configurations…** to launch the **Import and Export Configurations wizard**.

3. Select **Import the configuration from another instance** and click **Next**.

4. Click **Browse** to select the GFI LanGuard installation folder. The default location is `<Local Disk>\Program Files\GFI\ LanGuard <Version>`. Click **Next**.


Import and Export Configurations Wizard
Welcome to the Import and Export Configurations Wizard
Use this wizard to import or export GFI LanGuard configurations.
What do you want to do?
Export the desired configurations to a file
Export GFI LanGuard configuration to a file (.cfg)
Import the desired configurations from a file
Import GFI LanGuard configurations from a file (.cfg)
Import the configurations from another instance
Import GFI LanGuard configurations from another installation
< Back
Next >
Cancel

Screenshot 3: Import setting

5. Select which settings you want to import and click **Next**.

6. While importing, GFI LanGuard will ask you whether you want to override or keep your settings. Select one of the following options:

Table 9: Override options

Option	Description
Yes	Override the current setting with the imported setting.
No	Keep the current setting and ignore the imported setting.
Auto Rename	Rename the imported settings and keep the current settings.

7. Click **OK** when the import is ready.

2.4 Upgrading from previous versions

GFI LanGuard retains all settings and result information from any previous version of GFI LanGuard. This enables you to:

- Install GFI LanGuard without uninstalling the previous version.
- Import settings to GFI LanGuard from other instances.
- Deploy agents on the same machines where you have a previous version of GFI LanGuard installed.

> **Note**
>
> Software upgrades from versions older than GFI LanGuard 9 cannot be performed.

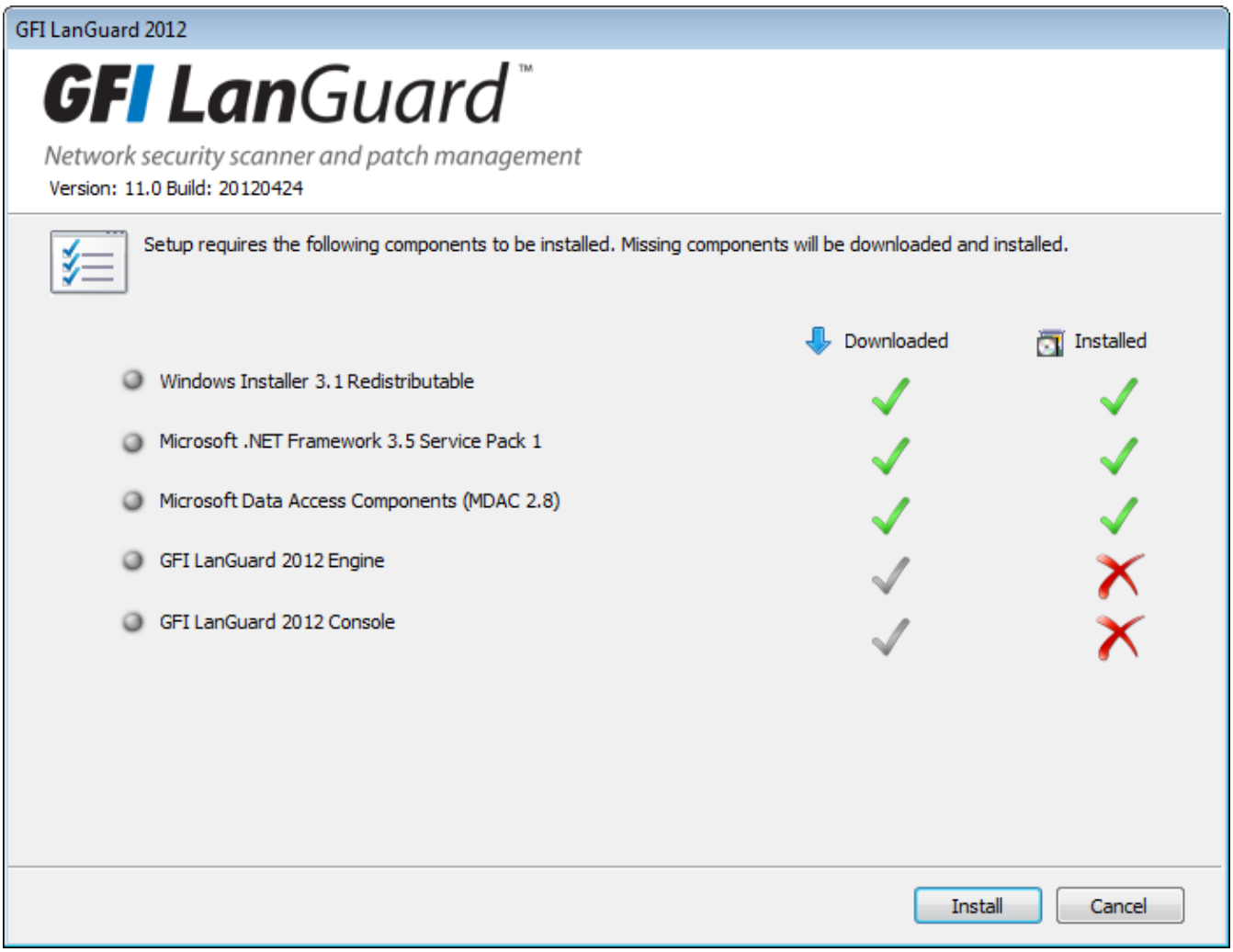
Note

License keys of earlier versions of GFI LanGuard are not compatible and must be upgraded to run GFI LanGuard.

To upgrade to a newer version:

1. Logon using administrator credentials on the machine where you wish to install GFI LanGuard.

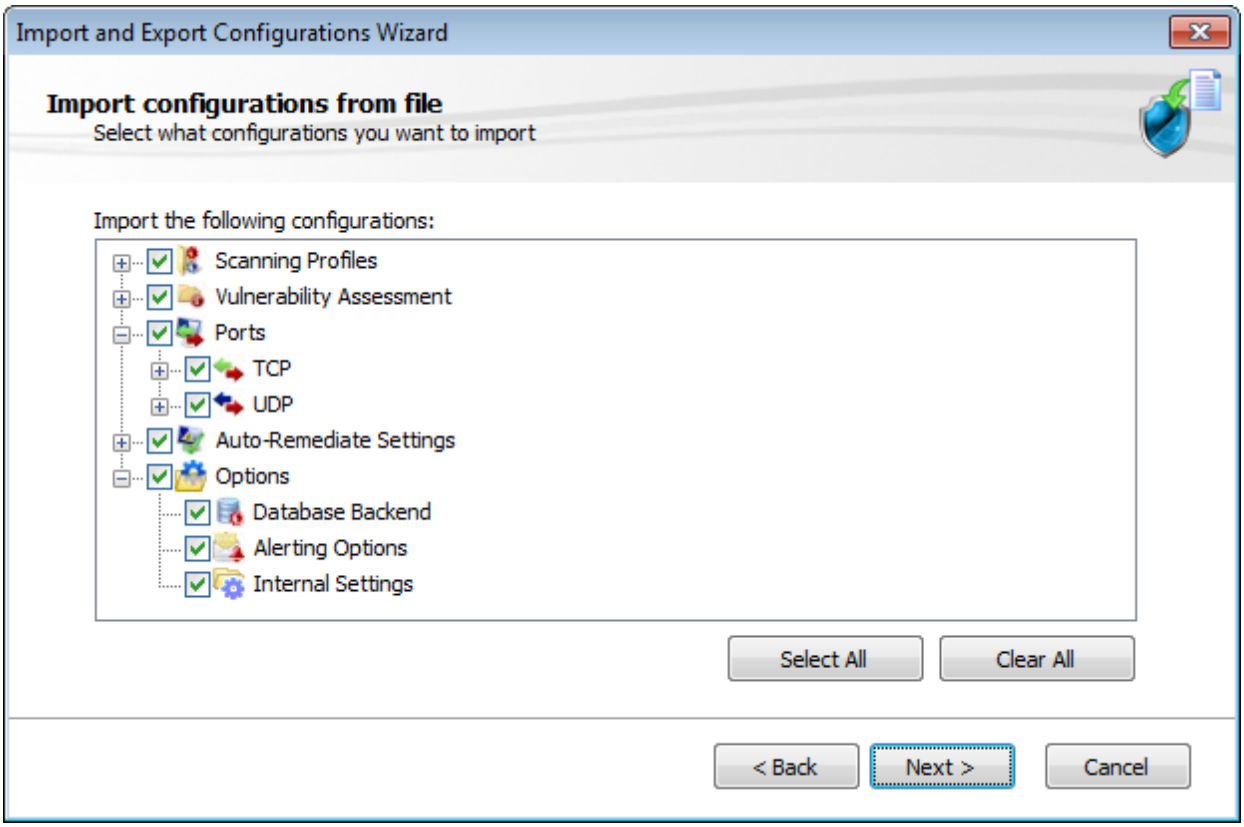
2. Launch GFI LanGuard installation.


GFI LanGuard 2012
GFI LanGuard
Network security scanner and patch management
Version: 11.0 Build: 20120424
Setup requires the following components to be installed. Missing components will be downloaded and installed.
Downloaded
Installed
Windows Installer 3.1 Redistributable
Microsoft .NET Framework 3.5 Service Pack 1
Microsoft Data Access Components (MDAC 2.8)
GFI LanGuard 2012 Engine
GFI LanGuard 2012 Console
Install
Cancel

Screenshot 4: Pre-requisite check dialog

3. The pre-requisite check dialog shows an overview of the status of the components required by GFI LanGuard to operate. Click **Install** to start the installation.

4. Follow the onscreen instructions to complete the upgrade.



Screenshot 5: Import and Export settings from a previous instance

5. Once GFI LanGuard is installed, it detects the previous installation and automatically launches the **Import and Export Configuration Wizard**. This enables you to export various configurations from the previous version and import them into the new one.

6. Select the configurations to import and click **Next** to finalize the import process.

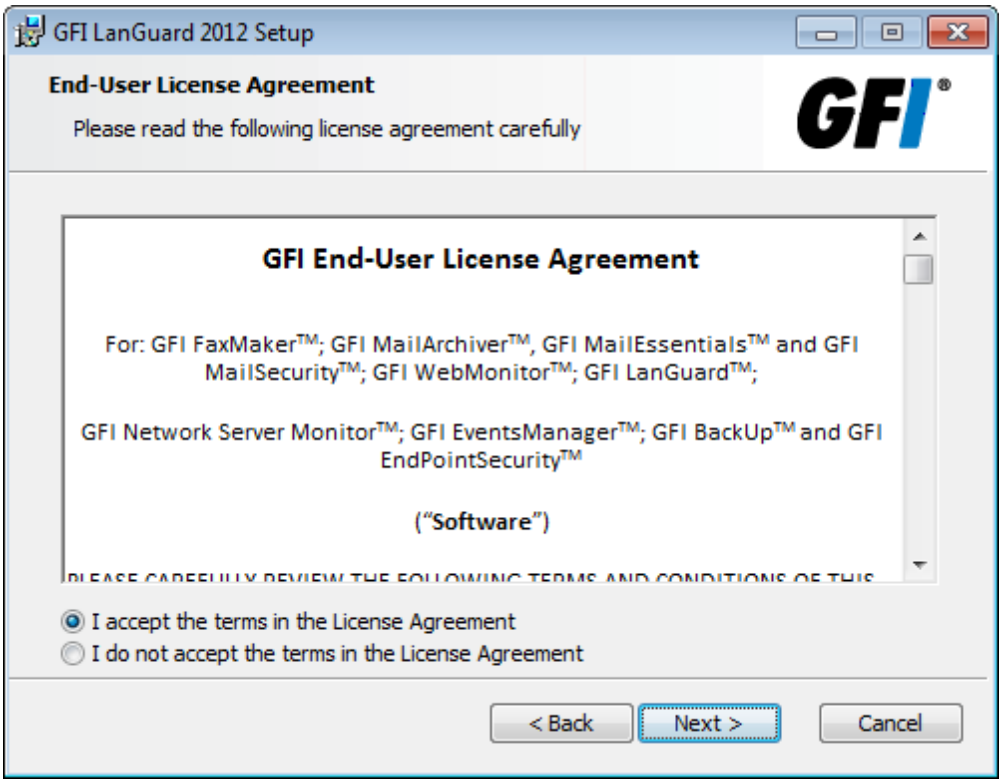
2.5 New installation

1. Logon using administrator credentials on the machine where GFI LanGuard will be installed.

2. Launch GFI LanGuard setup.

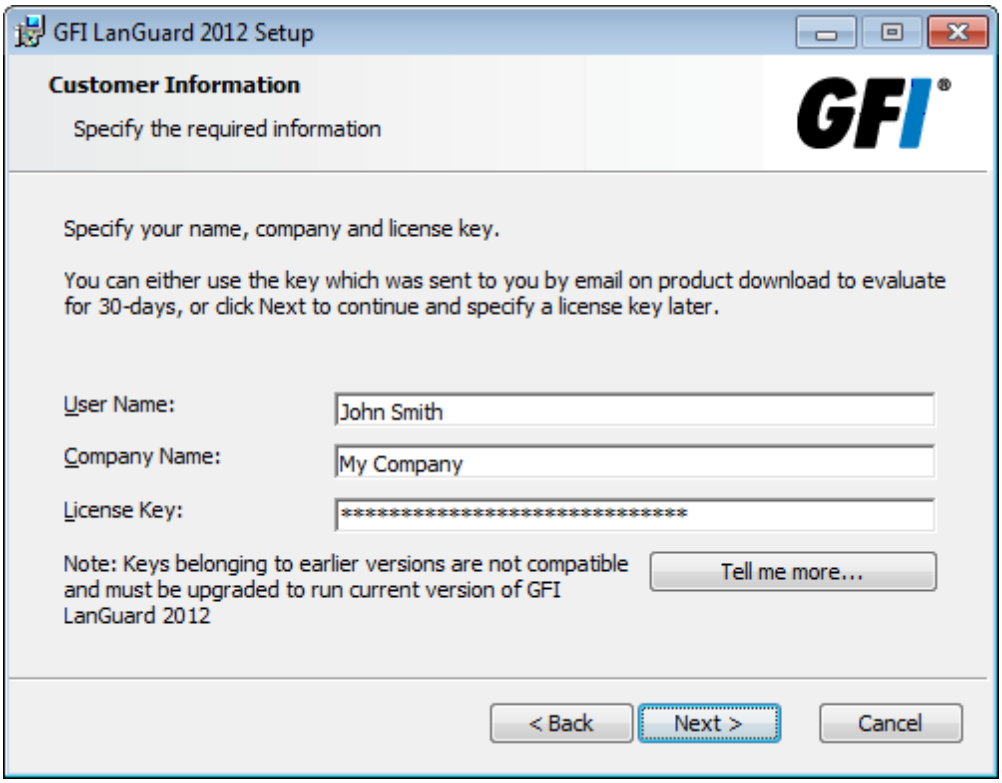
3. Click **Install** in the pre-requisite check window to download and install any missing required components.

4. In the GFI LanGuard welcome screen, click **Next**.


GFI LanGuard 2012 Setup
End-User License Agreement
Please read the following license agreement carefully
GFI End-User License Agreement
For: GFI FaxMaker™; GFI MailArchiver™, GFI MailEssentials™ and GFI MailSecurity™; GFI WebMonitor™; GFI LanGuard™;
GFI Network Server Monitor™; GFI EventsManager™; GFI BackUp™ and GFI EndPointSecurity™
("Software")
I accept the terms in the License Agreement
I do not accept the terms in the License Agreement
< Back
Next >
Cancel

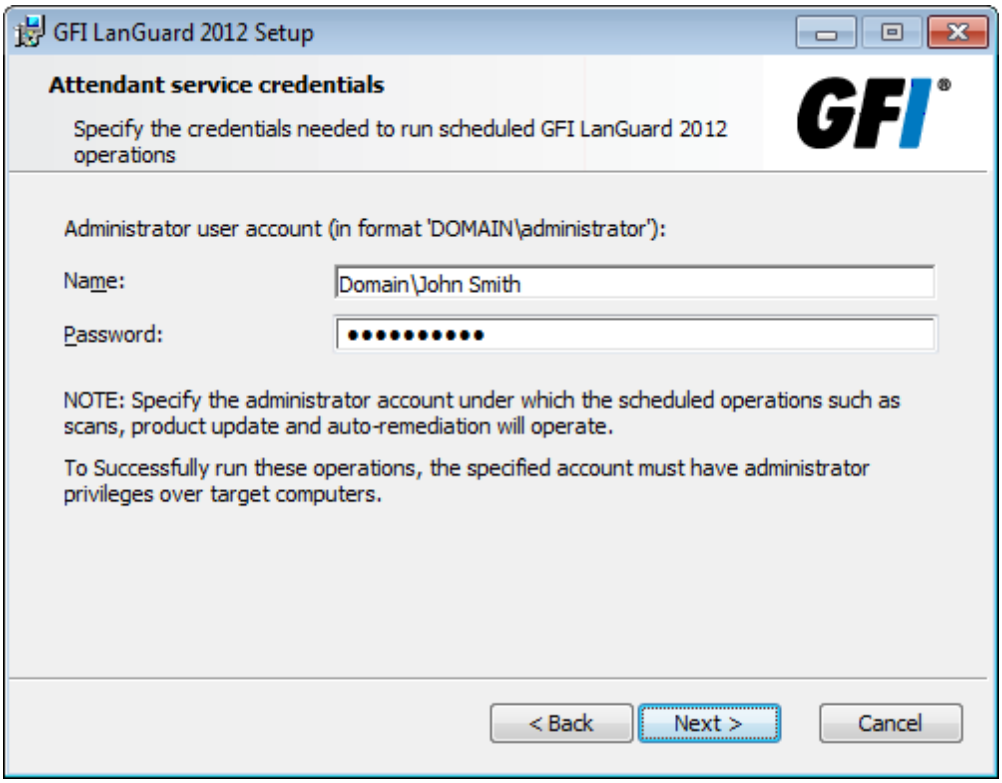
Screenshot 6: End-user license agreement

5. Read the licensing agreement carefully. To proceed with the installation, select **I accept the terms in the License Agreement** and click **Next**.


GFI LanGuard 2012 Setup
Customer Information
Specify the required information
Specify your name, company and license key.
You can either use the key which was sent to you by email on product download to evaluate for 30-days, or click Next to continue and specify a license key later.
User Name:
John Smith
Company Name:
My Company
License Key:
Note: Keys belonging to earlier versions are not compatible and must be upgraded to run current version of GFI LanGuard 2012
Tell me more...
< Back
Next >
Cancel

Screenshot 7: Specify user details and license key

6. Specify user details and enter license key. Click **Next**.


GFI LanGuard 2012 Setup
Attendant service credentials
Specify the credentials needed to run scheduled GFI LanGuard 2012 operations
GFI
Administrator user account (in format 'DOMAIN\administrator'):
Name:
Domain\John Smith
Password:
NOTE: Specify the administrator account under which the scheduled operations such as scans, product update and auto-remediation will operate.
To Successfully run these operations, the specified account must have administrator privileges over target computers.
< Back
Next >
Cancel

Screenshot 8: Attendant service credentials

7. Key in the administrator credentials and password. This will be used by the service under which scheduled operations will operate. Click **Next** to continue setup.

8. Click Install to install GFI LanGuard in the default location or click **Browse** to change path.

9. Click **Finish** to finalize installation.

When launched for the first time, GFI LanGuard automatically enables auditing on the local computer and scans the local computer for vulnerabilities. On completion, the GFI LanGuard **Home** page displays the vulnerability result.

Note

It is recommended that you test your installation after the product is installed. For more information, refer to Testing the installation (page 36).

Note

An Internet connection is required to download missing components.

Note

If the credentials keyed in are invalid, a message stating that this option can be skipped is displayed. It is highly recommended to provide a valid username and password and not to skip this option

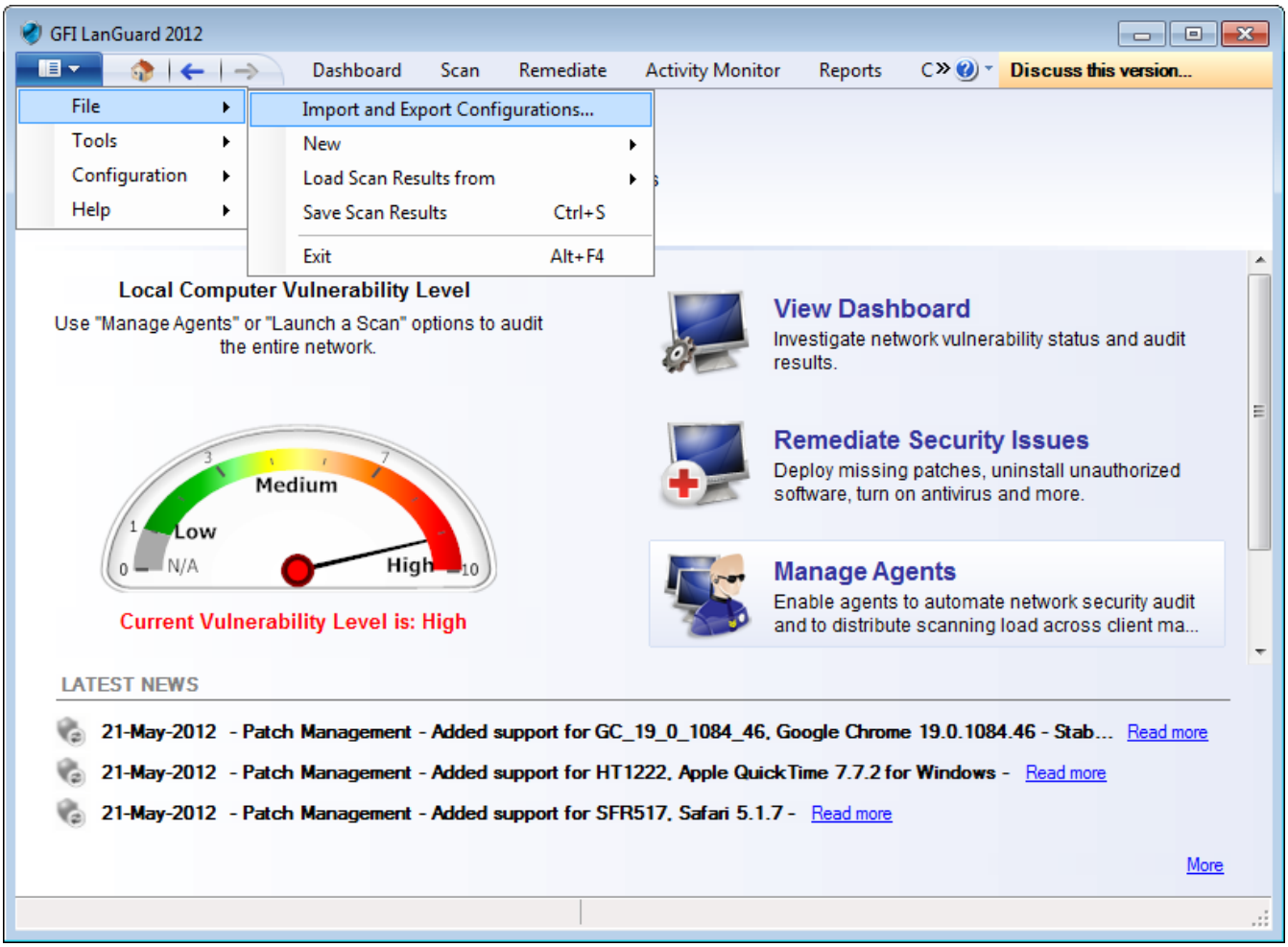
2.6 Post install actions

GFI LanGuard can be installed on a machine with an older version of GFI LanGuard without uninstalling it. This enables you to retain configuration settings and reuse them in the new version.

To import the settings from the earlier version:

1. Launch the GFI LanGuard management console from **Start > Programs > GFI LanGuard 2012 > GFI LanGuard 2012**.

2. Click the **GFI LanGuard button > File > Import and Export Configurations...** to launch the **Import and Export Configurations wizard**.


GFI LanGuard 2012
Dashboard
Scan
Remediate
Activity Monitor
Reports
Discuss this version...
File
Tools
Configuration
Help
Import and Export Configurations...
New
Load Scan Results from
Save Scan Results Ctrl+S
Exit Alt+F4
Local Computer Vulnerability Level
Use "Manage Agents" or "Launch a Scan" options to audit the entire network.
Medium
Low
High
N/A
Current Vulnerability Level is: High
View Dashboard
Investigate network vulnerability status and audit results.
Remediate Security Issues
Deploy missing patches, uninstall unauthorized software, turn on antivirus and more.
Manage Agents
Enable agents to automate network security audit and to distribute scanning load across client ma...
LATEST NEWS
21-May-2012 - Patch Management - Added support for GC_19_0_1084_46, Google Chrome 19.0.1084.46 - Stab... Read more
21-May-2012 - Patch Management - Added support for HT1222, Apple QuickTime 7.7.2 for Windows - Read more
21-May-2012 - Patch Management - Added support for SFR517, Safari 5.1.7 - Read more
More

Screenshot 9: Import and Export configurations

3. Select **Import the configuration from another instance** and click **Next**.

4. Click **Browse** to select the GFI LanGuard installation folder. The default location is:

- **64-bit machines (x64)** - `<Local Disk>\Program Files (x86)\GFI\ LanGuard <Version>`
- **32-bit machines (x86)** - `<Local Disk>\Program Files\GFI\ LanGuard <Version>`

5. Click **Next**.

6. Select the settings to import and click **Next**.

7. While importing, GFI LanGuard asks to override or keep existing settings. Select:

Table 10: Import override options

Option	Description
Yes	Override current setting with imported setting.
No	Keep current setting and ignore imported setting.
Auto Rename	Rename imported settings and keep the current settings.

8. Click **OK** when complete.

2.7 Testing the installation

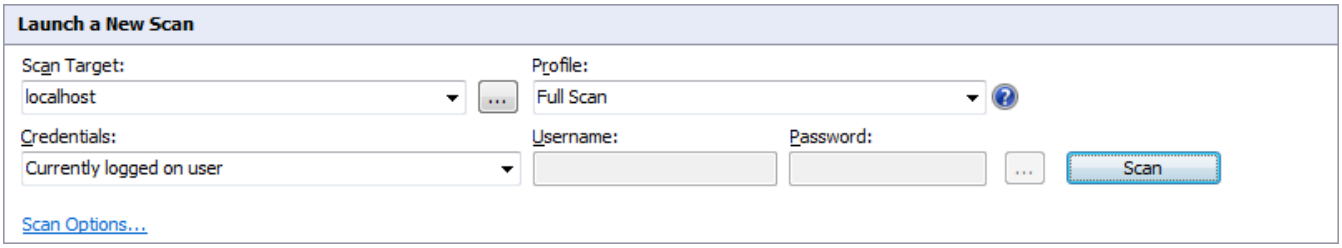
Once GFI LanGuard is installed, test your installation by running a local scan to ensure it installed successfully.

1. Launch GFI LanGuard.

GFI LanGuard 2012
Dashboard
Scan
Remediate
Activity Monitor
Reports
Discuss this version...
Welcome to GFI LanGuard 2012
GFI LanGuard 2012 is ready to audit your network for vulnerabilities
Medium
Low
High
N/A
Current Vulnerability Level is: High
Remediate Security Issues
Deploy missing patches, uninstall unauthorized software, turn on antivirus and more.
Manage Agents
Enable agents to automate network security audit and to distribute scanning load across client ma...
Launch a Scan
Manually set-up and trigger an agentless network security audit.
LATEST NEWS
21-May-2012 - Patch Management - Added support for GC_19_0_1084_46, Google Chrome 19.0.1084.46 - Stab... Read more
21-May-2012 - Patch Management - Added support for HT1222, Apple QuickTime 7.7.2 for Windows - Read more
21-May-2012 - Patch Management - Added support for SFR517, Safari 5.1.7 - Read more
More

Screenshot 10: Launch a scan

2. From GFI LanGuard home page, click **Launch a Scan**.



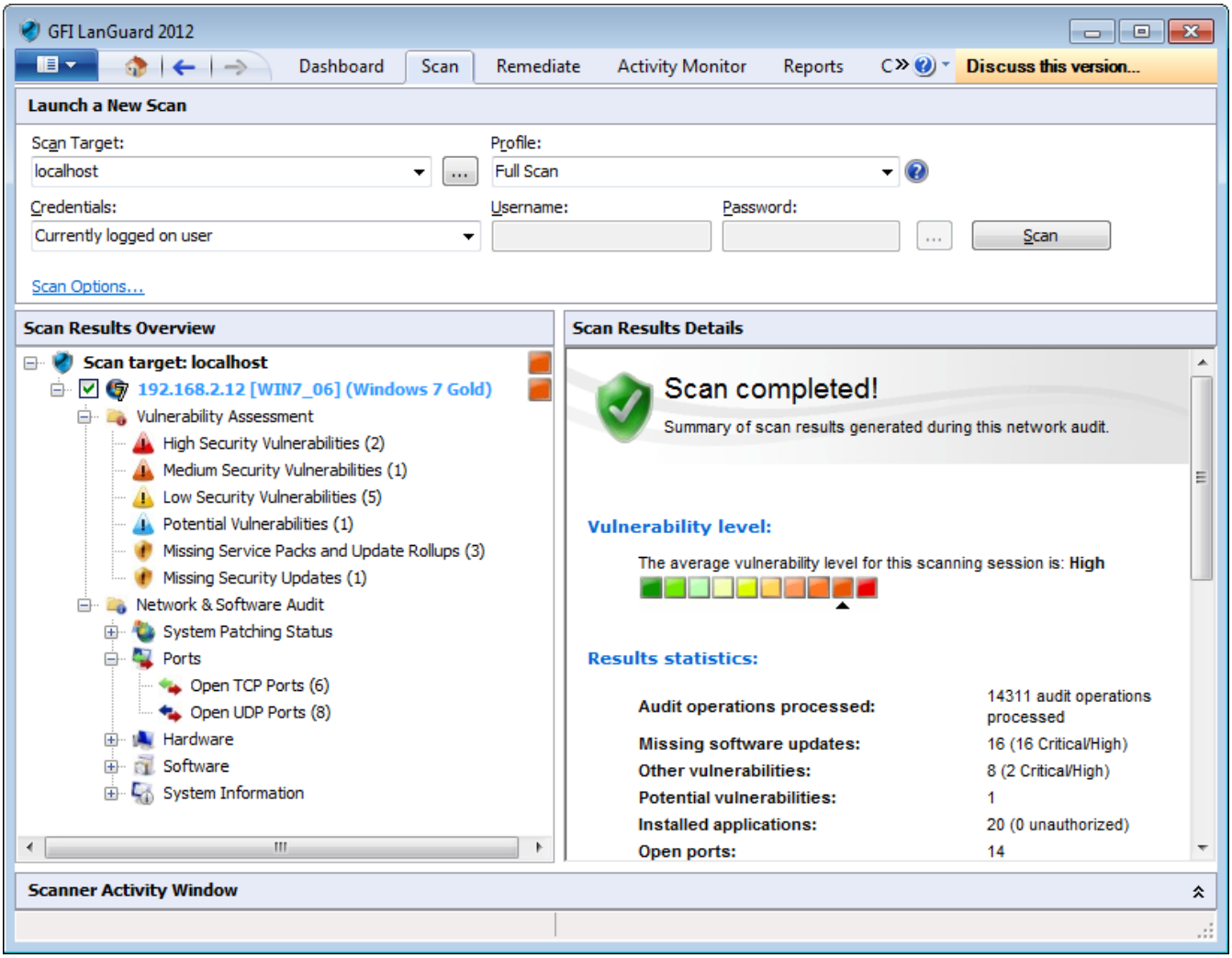
Screenshot 11: Launch a scan properties

3. From **Scan Target** drop-down menu, select **localhost**.

4. From **Profile** drop-down menu, select **Full Scan**.

5. Click **Scan** to start the scan on the local computer.

6. The scan progress is displayed in the **Scan** tab.



Screenshot 12: Scan results summary

7. On completion, the **Progress** section will display an overview of the scan result.

8. Use the **Scan Results Details** and **Scan Results Overview** to analyze the scan result. For more information, refer to Interpreting manual scan results (page 104).

3 Achieving Results

This chapter provides you with step by step instructions about how to strengthen your network's security and integrity using GFI LanGuard. This chapter helps you achieve positive patch management, vulnerability management and legal compliance results, while ensuring that your network is protected using the most up-to-date vulnerability detection methods and techniques.

Topics in this chapter:

3.1 Effective Vulnerability Assessment 38

3.2 Effective Patch Management 39

3.3 Using GFI LanGuard for asset tracking 40

3.4 Up to date network and software analysis 41

3.5 Compliance with PCI DSS 42

3.1 Effective Vulnerability Assessment

For an effective vulnerability management strategy follow the steps described below:

1. Keep GFI LanGuard up to date.

- Make sure that the machine where GFI LanGuard is installed has Internet access. GFI LanGuard performs daily checks for updated information.
- If a proxy server is used, refer to Configure Proxy Settings.
- If Internet access is not available on the machine where GFI LanGuard is installed, refer to Installing program updates manually.

2. Perform security audits on a regular basis.

- Agent Scheduled Scans
- Manual Scans
- Scheduled Scans

3. Deploy missing security updates and remove unauthorized applications.

- Configure Agents Auto-Remediation
- Configure Automatic Remediation
- Deploying Security Patches and Service Packs
- Uninstalling Software Patches and Service Packs

4. Investigate and remediate other security issues.

- Deploying Custom Software
- Malware Protection Actions
- Uninstalling Custom Applications
- Using Remote Support

---

5. Check network security status.

- Use the Dashboard to monitor and view the status of your network. To learn more about the Dashboard, refer to Using the Dashboard

---

3.2 Effective Patch Management

GFI LanGuard enables you to manage patch deployment on your network.

GFI LanGuard can support patch updates for the following:

- Windows® operating systems
- Microsoft® applications
- Most commonly used third party applications (Adobe products, Java runtimes and web browsers)
- MAC operating systems

---

1. Use the Dashboard to view missing patches:

- Patches View

---

2. Customize the patches scanning profile:

- Configuring Patches

---

3. Remediate vulnerabilities related to missing patches:

- Deploying Security Patches and Service Packs
- Uninstalling Software Patches and Service Packs

3.3 Using GFI LanGuard for asset tracking

Unmanaged or forgotten devices are a security risk. Perform the following steps to track unmanaged and forgotten devices:

1. Automatically discover new devices in your network

GFI LanGuard automatically detects new computers on your network:

- Enumerate Computers
- Network discovery

2. Deploy agents on new discovered computers

- Deploying Agents
- Deploy Agents Manually
- Agent Properties
- Agents Settings

3. Use the Dashboard to view vulnerabilities related to the new computers

- Overview
- Computers View
- Vulnerabilities View
- Software View
- Hardware View
- System Information View

3.4 Up to date network and software analysis

Network analysis enables you to learn more what is happening in your network because it detects the configurations and applications that are posing a security risk on your network. Such issues can be identified using the following functions:

GFI LanGuard views and tools

- Software View - Get a detailed view of all the applications installed in the network.
- Hardware View - Check the hardware inventory of the network.
- System Information - View security sensitive details about the systems present in the network.
- History - Get a list of security sensitive changes that happened in the network
- Software Audit - Generate a comprehensive report about the applications installed in the network.

Remediate issues

- Remediate Vulnerabilities
- Configure Unauthorized applications Auto-Uninstall
- Deploying Custom Software
- Uninstalling Custom Applications
- Using Remote Support

3.5 Compliance with PCI DSS

Be fully compliant with PCI DSS, the strict security standards drawn up by the world's major credit card companies. In providing complete vulnerability management coupled with extensive reporting, GFI LanGuard is an essential solution to assist with your PCI compliance program. To learn more about how to be compliant with PCI DSSuse the following links:

Registration form for PCI DSS Compliance and GFI Software Products.

» http://go.gfi.com/?pageid=PCIDSS_Compliance_Whitepaper

Best practices

» Perform regular vulnerability assessments. Refer to Scanning your network.

» Remediate vulnerabilities and deploy missing patches. Refer to Remediate Vulnerabilities.

» Generate reports and view your infrastructure status. Refer to Reporting.

» Ensure that antivirus and antispyware software is installed and running on target computers. To achieve this, run a scan on your targets using the **Software Audit** scanning profile, from the Network & Software Audit group. For more information, refer to Available Scanning Profiles (page 64).

» Ensure that personal firewall is installed and running on target computers. For more information, refer to Manual scans (page 66).

» Ensure that encryption software is installed on your network. For more information, refer to Manual scans (page 66).

Other GFI products that can help you achieve compliance

» GFI VIPRE – antivirus, antispyware and personal firewall solution

» GFI EventsManager – log management solution

» GFI EndPointSecurity – device blocking solution

4 Managing Agents

GFI LanGuard can be configured to deploy agents automatically on newly discovered machines or manually, on selected computers. Agents enable faster audits and drastically reduce network bandwidth utilization. When using Agents, audits are performed using the scan target's resource power. Once an audit is finished, the results are transferred to GFI LanGuard in an XML file.

Topics in this chapter:

4.1 Deploying Agents 43

4.2 Deploy Agents manually 45

4.3 Agent properties 47

4.4 Agents settings 52

4.5 Configuring Relay Agents 53

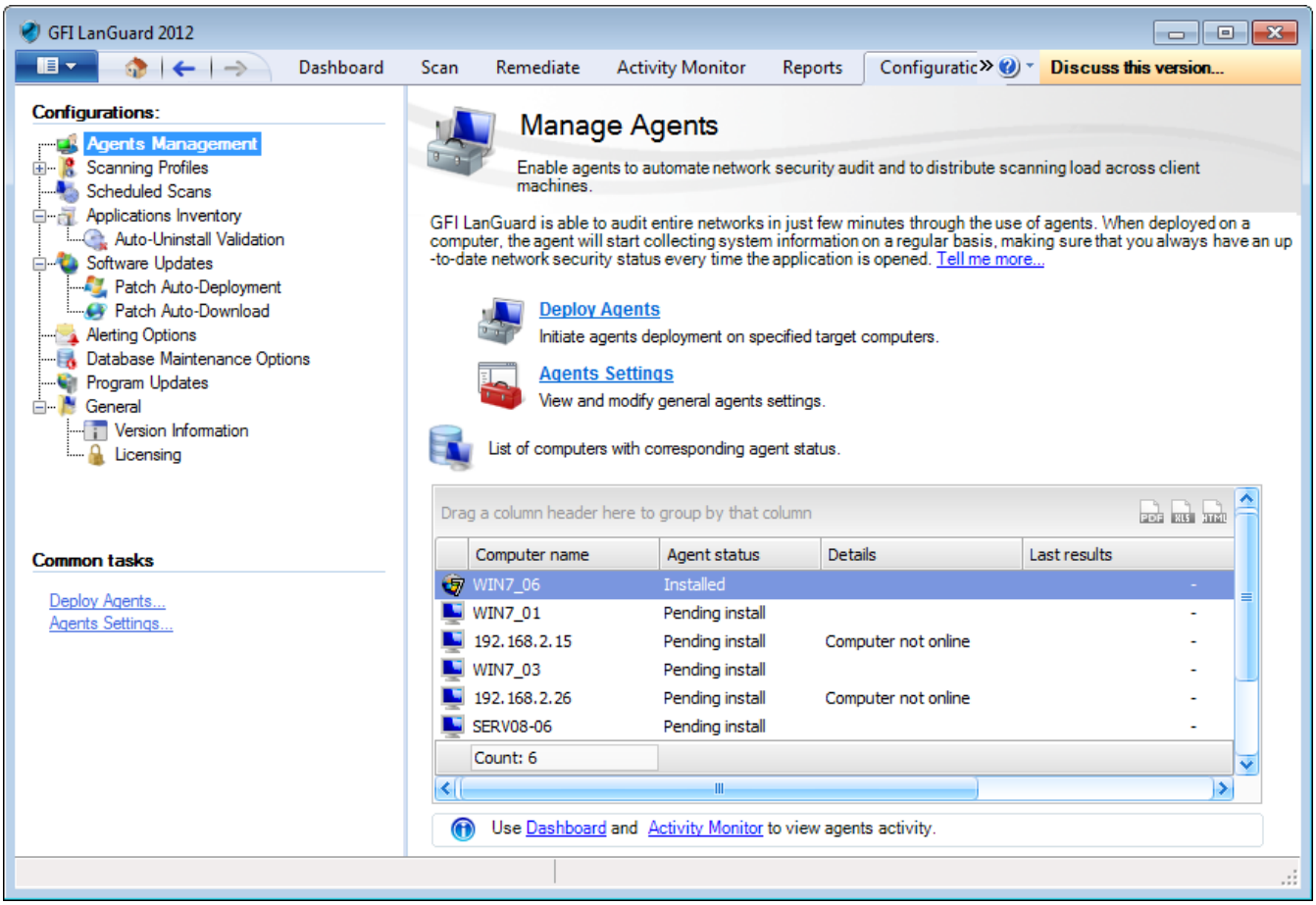
4.6 Managing Agent groups 61

4.1 Deploying Agents

To deploy GFI LanGuard Agents on network computers:

1. Launch GFI LanGuard.

2. From the **Home** menu, select **Manage Agents**. Alternatively, click **Configuration tab > Agents Management**.


GFI LanGuard 2012
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuratic
Discuss this version...
Configurations:
Agents Management
Scanning Profiles
Scheduled Scans
Applications Inventory
Auto-Uninstall Validation
Software Updates
Patch Auto-Deployment
Patch Auto-Download
Alerting Options
Database Maintenance Options
Program Updates
General
Version Information
Licensing
Common tasks
Deploy Agents...
Agents Settings...
Manage Agents
Enable agents to automate network security audit and to distribute scanning load across client machines.
GFI LanGuard is able to audit entire networks in just few minutes through the use of agents. When deployed on a computer, the agent will start collecting system information on a regular basis, making sure that you always have an up-to-date network security status every time the application is opened. Tell me more...
Deploy Agents
Initiate agents deployment on specified target computers.
Agents Settings
View and modify general agents settings.
List of computers with corresponding agent status.
Drag a column header here to group by that column
Computer name
Agent status
Details
Last results
WIN7_06 Installed -
WIN7_01 Pending install -
192.168.2.15 Pending install Computer not online -
WIN7_03 Pending install -
192.168.2.26 Pending install Computer not online -
SERV08-06 Pending install -
Count: 6
Use Dashboard and Activity Monitor to view agents activity.

Screenshot 13: Manage agents

3. From **Common Tasks**, click **Deploy Agents** to select the target scan computers and click **Next**. Select one of the options described below:

Table 11: Target selection

Option	Description
Local Domain	Deploy agents on all reachable computers within the same workgroup / domain where GFI LanGuard is installed. No further configuration is required in **Define target** step.
Custom	Deploy agents on specific computers or group of computers. Add new rules to search or specify target scan computers.

4. If **Custom** option is selected, click **Add new rule** and select the **Rule type** described below:

Table 12: Custom rules options

Rule type	Description
Computer name is	Manually enter a computer name or import the names from a saved text (.txt) file. Click **Select** and manually select computers from the list, or click **Import** and specify the text file location.
Domain name is	Select domains from the list of reachable domains.
Organization unit is	Select computers from one or more reachable organization units. Use the following options: » **Retrieve** - Specify the user name and password to retrieve the list » **Refresh** - Refresh the list of domains and Organization Units » **Add** - Manually add an Organization Unit.

Repeat step 4 for each rule. Once completed, click **OK**.

5. From **Deploy Agents** dialog, click **Next**.

6. (Optional) Select **Authenticate** using checkbox to specify alternate credentials.

7. (Optional) Click **Advanced Settings**, and configure the settings in the following tabs:

Table 13: Deploy Agents: Advanced Settings

Tab	Description
General	Configure the schedule for when GFI LanGuard automatically scans for new machines in the network perimeter where agents are enabled.
Audit Schedule	Configure how often the agent audits the host computer (where the agent is installed). Select the recurrence pattern, the time the audit will start and the scan profile to use.
Auto remediation	Configure GFI LanGuard to automatically download and install missing patches and service packs. Uninstall unauthorized applications on the scanned computers. For more information, refer to Automatic Remediation (page 116).

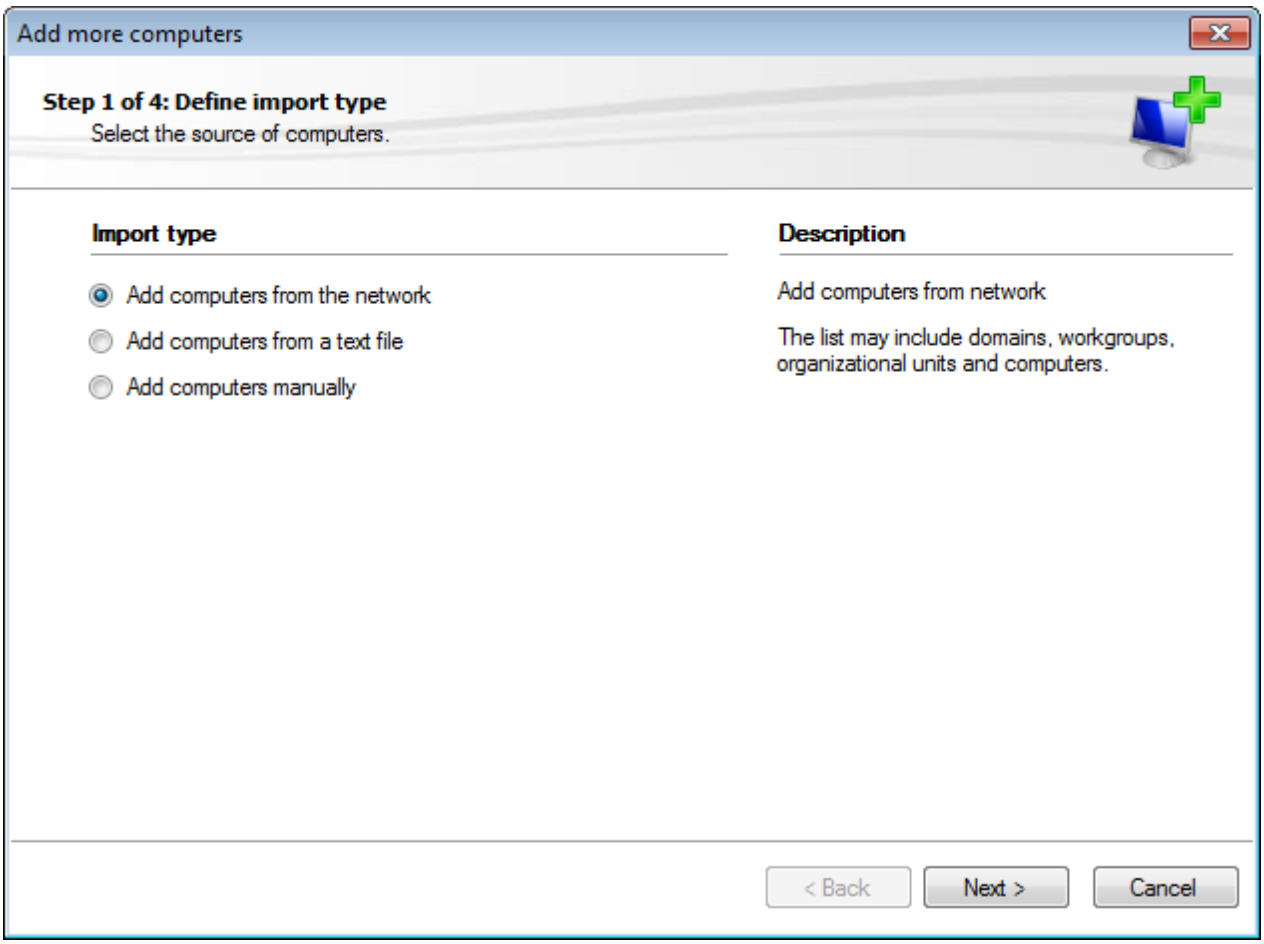
8. Click **Next** and **Finish** to complete agent deployment.

4.2 Deploy Agents manually

To deploy agents manually:

1. Launch GFI LanGuard and select **Dashboard**.

2. From **Common Tasks**, select **Add more computers**.


Add more computers
Step 1 of 4: Define import type
Select the source of computers.
Import type
Add computers from the network
Add computers from a text file
Add computers manually
Description
Add computers from network
The list may include domains, workgroups, organizational units and computers.
< Back
Next >
Cancel

Screenshot 14: Add more computers - Select import type

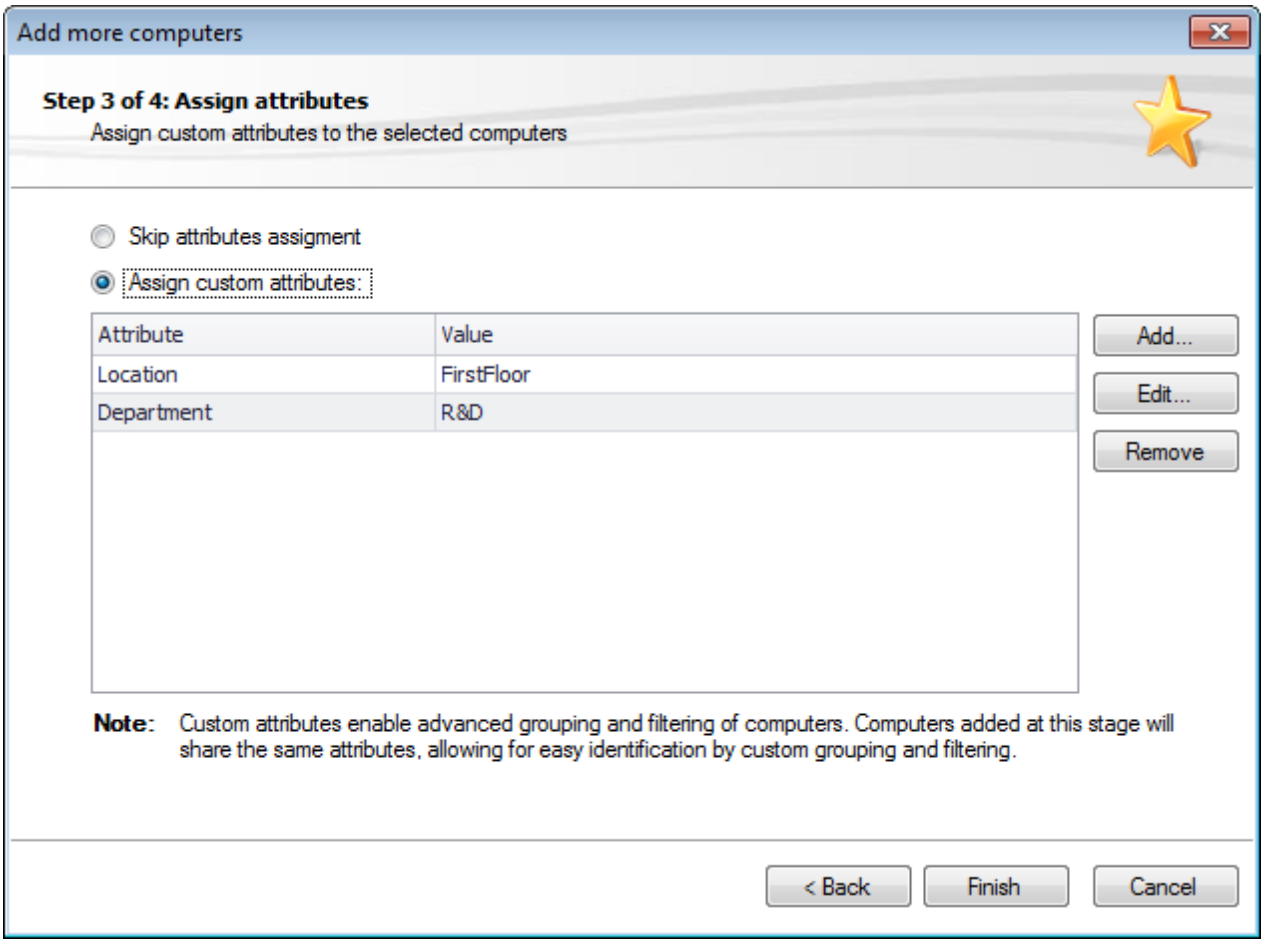
3. From the Add more computers wizard, select one of the following options:

Table 14: Add more computers wizard

Option	Description
Add computers from the network	Select domains, organizational units and computers from the list. Use the **Add domain** to add a new domain to the list of computers.

Option	Description
Add computers from a text file	Import computer list from text file. Click **Browse** and locate the text file containing the list of computers.
Add computers manually	Manually create a list of computers. Use the **Add** and **Remove** buttons to add and remove computers from the list. Use the **Import** and **Export** buttons to import and export the list from\to a text file.

Click **Next**.



Screenshot 15: Add more computers - Assign attributes to new computers

4. Custom attributes can be assigned to specific computers to ease grouping and filtering. From the **Assign attributes** wizard, configure the following:

Table 15: Attributes settings

Option	Description
Skip attributes assignment	No attributes are added to the computers list.
Assign custom attributes	Assign attributes to the list of computers. Click the **Add** button and specify the new attribute name and value. **Note** When importing a list of computers from a text file, GFI LanGuard automatically assigns the file name as an attribute (File) to the imported list.

5. Click **Finish**.

> **Note**
>
> If the selected computers have different login credentials from the GFI LanGuard machine, GFI LanGuard launches a dialog that enables you to specify valid credentials.

6. Once the computers are added to the list, click **Close**.

7. From the computer tree, right-click the newly added computers and select the computer where to deploy the agent and from the **Agent Status** click **Deploy Agent**.

8. Configure the Agent properties. For more information, refer to Agent properties (page 47).

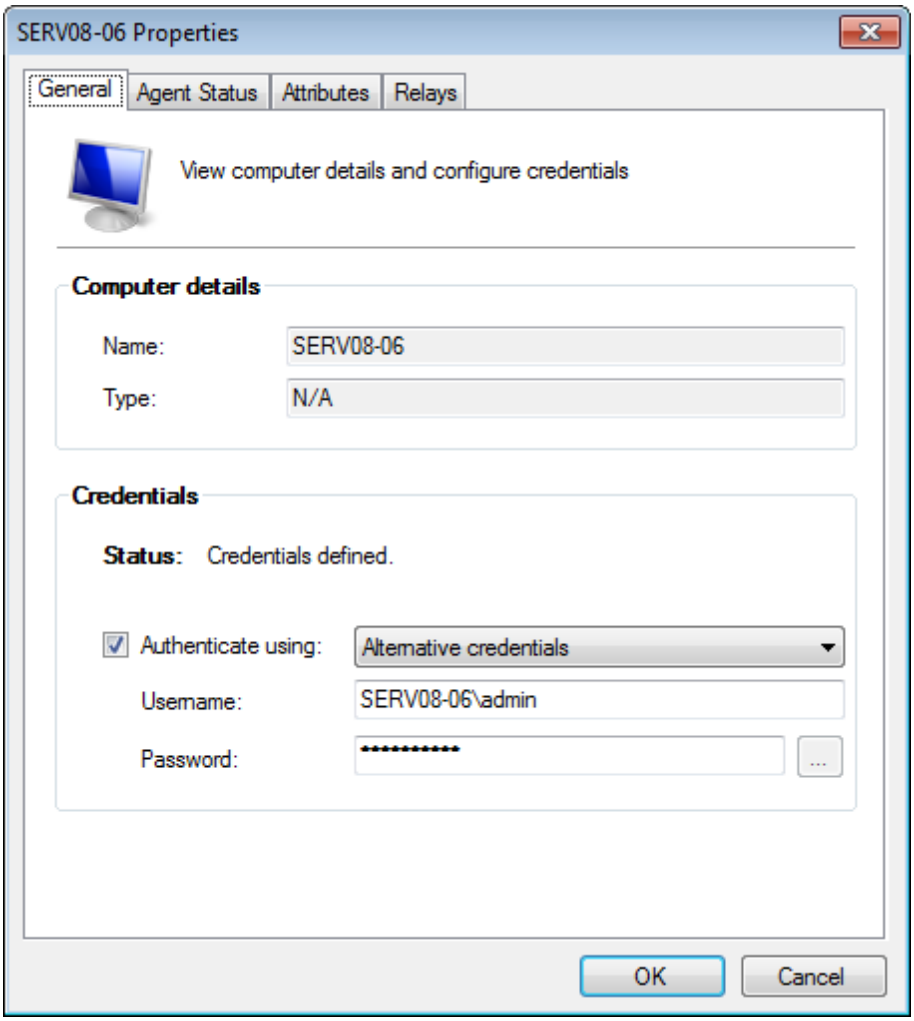
4.3 Agent properties

To modify agent properties:

1. Click **Configuration** tab > **Agents Management**.

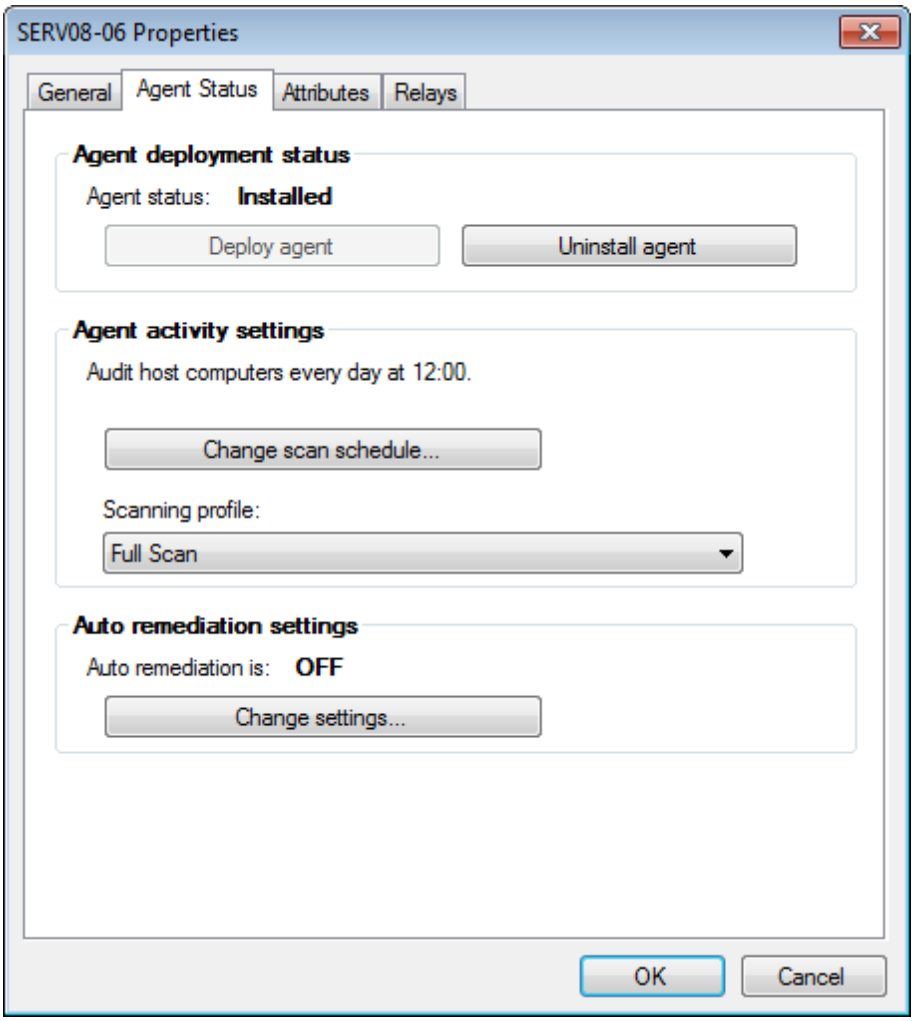
2. From the right pane, right-click an agent and select **Properties**.

> **Note**
>
> The **Properties** dialog can also be accessed from the computer tree within the **Dashboard**. Right-click a computer or a group and select **Properties**.



Screenshot 16: Agent Properties - General tab

3.(Optional) From **General** tab, specify the name, type and authentication method for the selected agent.



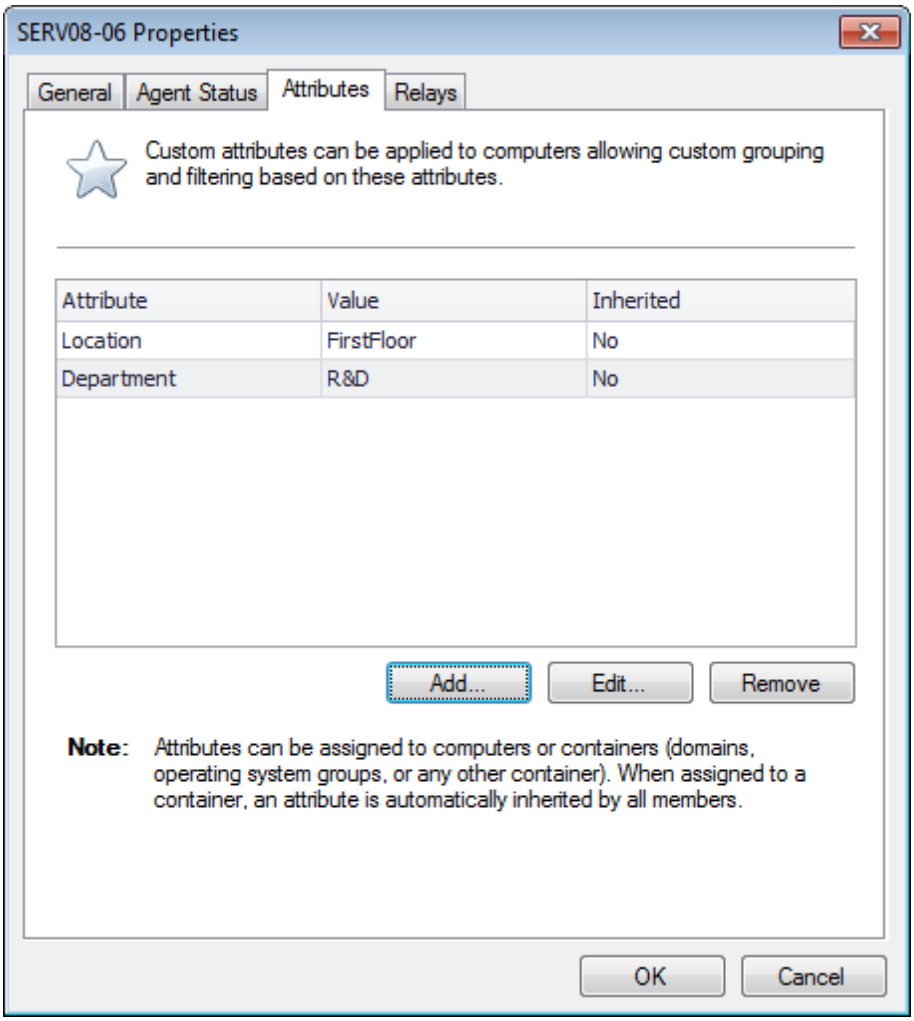
Screenshot 17: Agent Properties - Agent Status tab

4. From **Agent Status** tab, enable/disable agent deployment by clicking **Deploy agent** or **Disallow agent installation**.

5. Click **Change scan schedule…** to configure the selected agent's scan schedule.

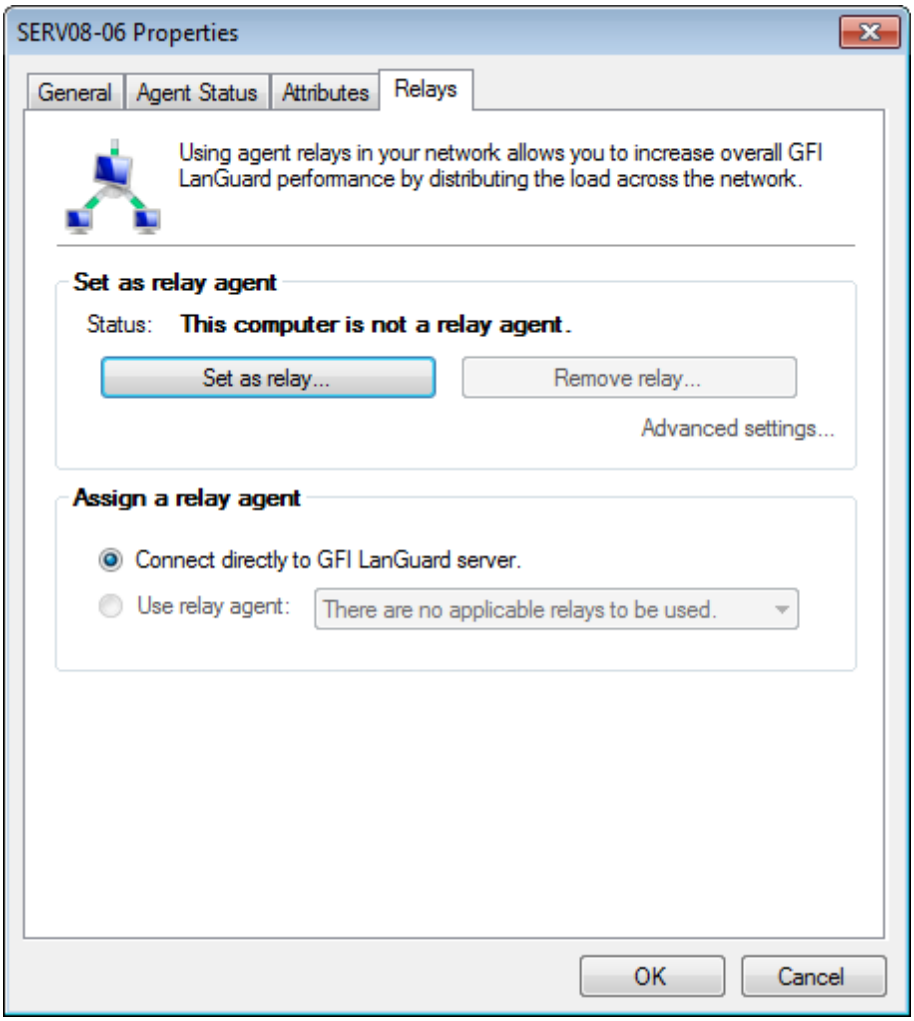
6. From **Scanning profile** drop-down menu, select the active scan profile.

7. From **Auto remediation settings**, click **Change settings…** to enable/disable agent auto-remediation. For more information, refer to Configuring auto-remediation options (page 125).



Screenshot 18: Agent Properties - Attributes tab

8. Click **Attributes** tab to manage the attributes assigned to the selected computer. Use the **Add**, **Edit** and **Remove** buttons to manage attributes.


SERV08-06 Properties
General
Agent Status
Attributes
Relays
Using agent relays in your network allows you to increase overall GFI LanGuard performance by distributing the load across the network.
Set as relay agent
Status: This computer is not a relay agent.
Set as relay...
Remove relay...
Advanced settings...
Assign a relay agent
Connect directly to GFI LanGuard server.
Use relay agent:
There are no applicable relays to be used.
OK
Cancel

Screenshot 19: Agent Properties - Relays tab

9. Click **Relays** tab to configure agent relays. Relays enable computers other than the one hosting GFI LanGuard to act as GFI LanGuard server. This helps you load-balance traffic directed to that machine and optimize network scanning performance.

10. Configure the options described below:

Table 16: Agent relay options

Option	Description
Set as relay	Set the selected computer as a relay agent. The selected computer will send product updates and patches to other agents to reduce the load from the GFI LanGuard machine. Click **Set as relay...** and follow the configuration wizard.
Remove relay	Remove the relay agent role from the selected computer. Click **Remove relay...** and follow the configuration wizard.
Connect directly to GFI LanGuard server	The selected computer will download product updates and patches from the GFI LanGuard server.
Use relay agent	The selected computer will use a relay agent to download product updates and patches. Select the relay agent to use from the drop down list.

11. (Optional) Click **Advanced Settings** and configure the following options:

Table 17: Relay agent advanced settings

Option	Description
Caching directory	All patches and updates are stored in this location before installation on the client computer.
Port where to serve	The port used by the relay agent to serve requests.

Option	Description
Address where to server	The address used by client computers to connect to the relay agent (By default the DNS host name is used).

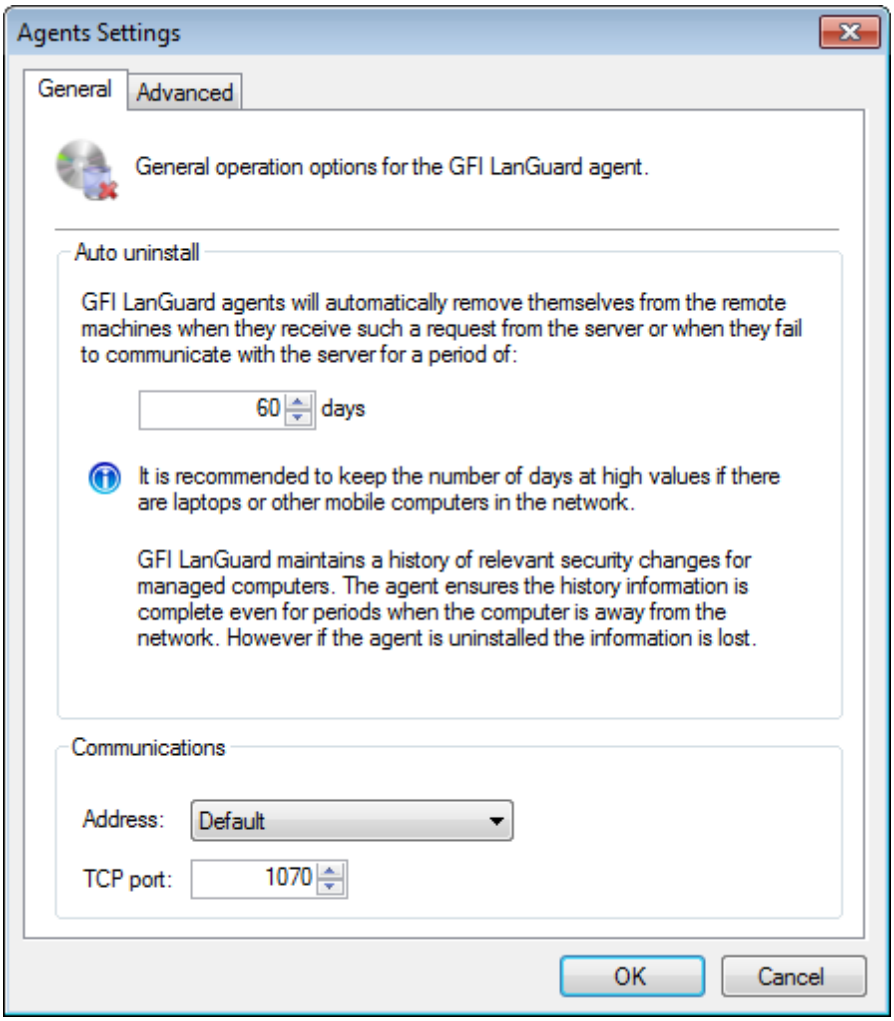
12. Click **OK** twice.

4.4 Agents settings

To configure additional agents' settings:

1. From **Configuration** tab, select **Agents Management**.

2. Click **Agents Settings**.

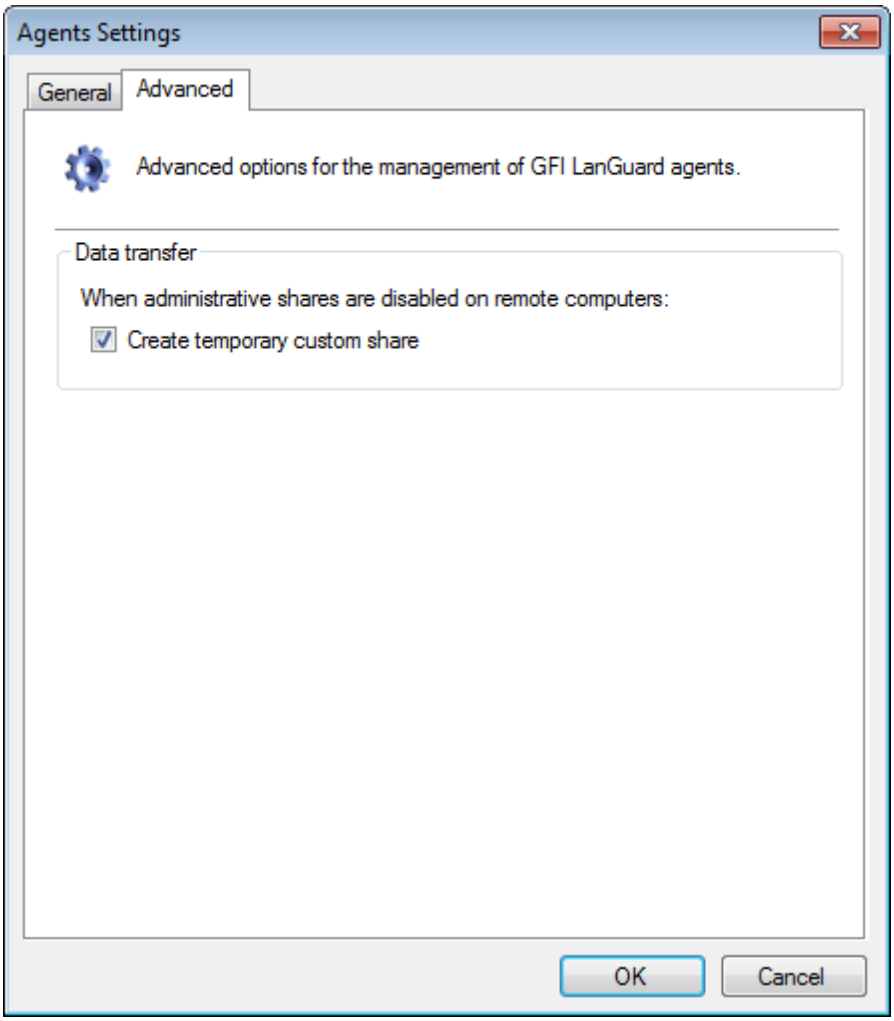

Agents Settings
General
Advanced
General operation options for the GFI LanGuard agent.
Auto uninstall
GFI LanGuard agents will automatically remove themselves from the remote machines when they receive such a request from the server or when they fail to communicate with the server for a period of:
60
days
It is recommended to keep the number of days at high values if there are laptops or other mobile computers in the network.
GFI LanGuard maintains a history of relevant security changes for managed computers. The agent ensures the history information is complete even for periods when the computer is away from the network. However if the agent is uninstalled the information is lost.
Communications
Address:
Default
TCP port:
1070
OK
Cancel

Screenshot 20: Agent Settings - General tab

3. Configure the options described below:

Table 18: Agents settings

Option	Description
Auto uninstall	Set the number of days after which GFI LanGuard Agents automatically uninstall themselves if the host computer is unresponsive for the set period of days.
Agents report using	Configure the port and IP address used by agents to communicate and report status to GFI LanGuard. When GFI LanGuard machine has multiple IP addresses and Default setting is selected, GFI LanGuard automatically selects the IP address to use.



Screenshot 21: Agent Settings - Advanced tab

4. (Optional) Click **Advanced** tab and select **Create temporary custom share**. When this option is enabled and administrative shares are disabled on agent machines, GFI LanGuard creates a temporary shared folder for transferring information.

5. Click **OK** to save and close dialog.

WARNING

Communication on TCP port **1070** must be enabled in Windows firewall for GFI LanGuard Agents to send data to GFI LanGuard.

4.5 Configuring Relay Agents

In larger networks you may experience some performance degradation due to the number of scan targets and the volume of data transferred to the GFI LanGuard server component. This results in slower scan-speed and retrieval of scan data.

To help you avoid performance issues and apply load balancing techniques, GFI LanGuard enables you to configure Agents to act as a relay of the server. Agents that are configured as Relay Agents download patches and definitions directly from GFI LanGuard server and forward them to client computers (which can be Agent-based and Agent-less computers). The main advantages of using Relay Agents are:

- Reduced bandwidth consumption in local or geographically distributed networks. If a Relay Agent is configured on each site, a patch is only downloaded once and distributed to client computers
- Reduced performance load from the GFI LanGuard server component and distributed amongst relay agents
- Using multiple Relay Agents, increases the number of devices that can be protected simultaneously.

Relay Agents behave the same as GFI LanGuard and are able to manage security auditing and remediation operations on other scan targets connected to the relay.

Refer to the following sections for information about:

- Configuring an Agent as a Relay
- Configuring Relay Agent advanced options
- Connecting computers to a Relay Agent

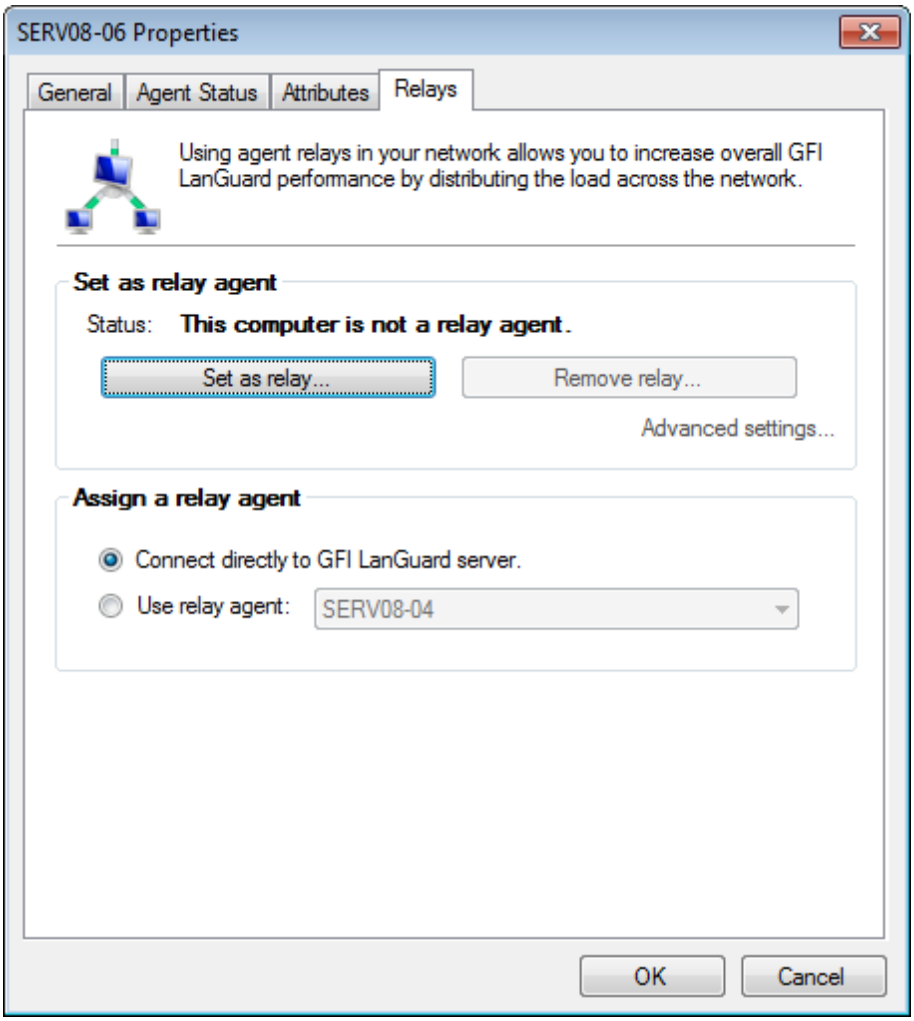
4.5.1 Configuring an Agent as a Relay

To configure an Agent to act as a Relay Agent:

> **Note**
>
> The machine where GFI LanGuard is installed cannot be configured as a Relay Agent. The **Relays** tab from the Agent's **Properties** dialog is missing for the GFI LanGuard host.

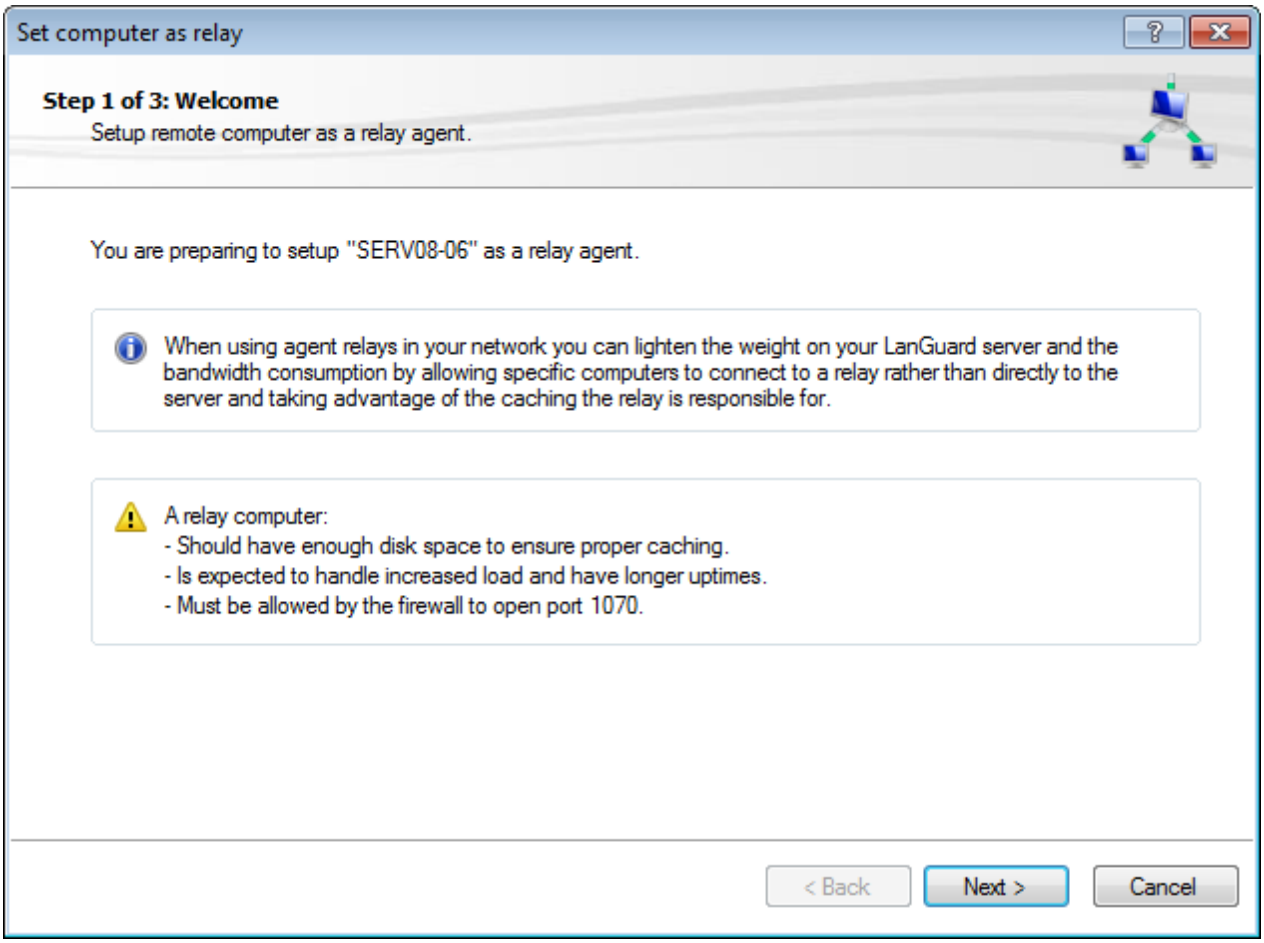
1. Open GFI LanGuard.
2. Click **Configuration** tab > **Agents Management**.
3. Right-click on the Agent you want to configure and select **Properties**. This opens the Agent's **Properties** dialog.

> **Note**
>
> Alternatively, right-click on an computer/group from the computer tree and select **Properties**.



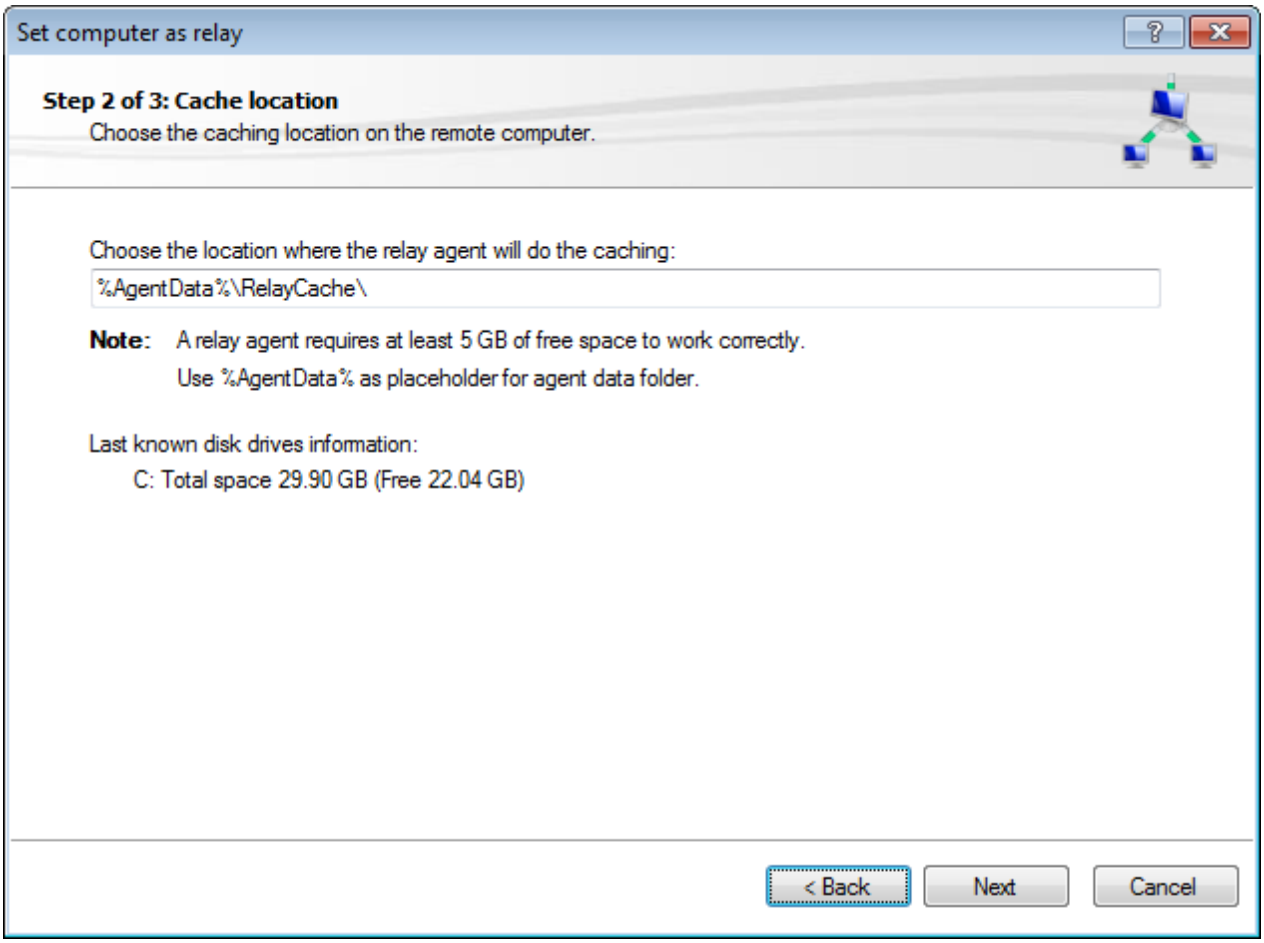
Screenshot 22: Agent Properties dialog

4. From the **Relays** tab, click **Set as relay...**


Set computer as relay
Step 1 of 3: Welcome
Setup remote computer as a relay agent.
You are preparing to setup "SERV08-06" as a relay agent.
When using agent relays in your network you can lighten the weight on your LanGuard server and the bandwidth consumption by allowing specific computers to connect to a relay rather than directly to the server and taking advantage of the caching the relay is responsible for.
A relay computer:
- Should have enough disk space to ensure proper caching.
- Is expected to handle increased load and have longer uptimes.
- Must be allowed by the firewall to open port 1070.
< Back
Next >
Cancel

Screenshot 23: Set computer as relay wizard

5. Carefully ready the warning about resource requirements for the computer running a Relay Agent. Click **Next**.

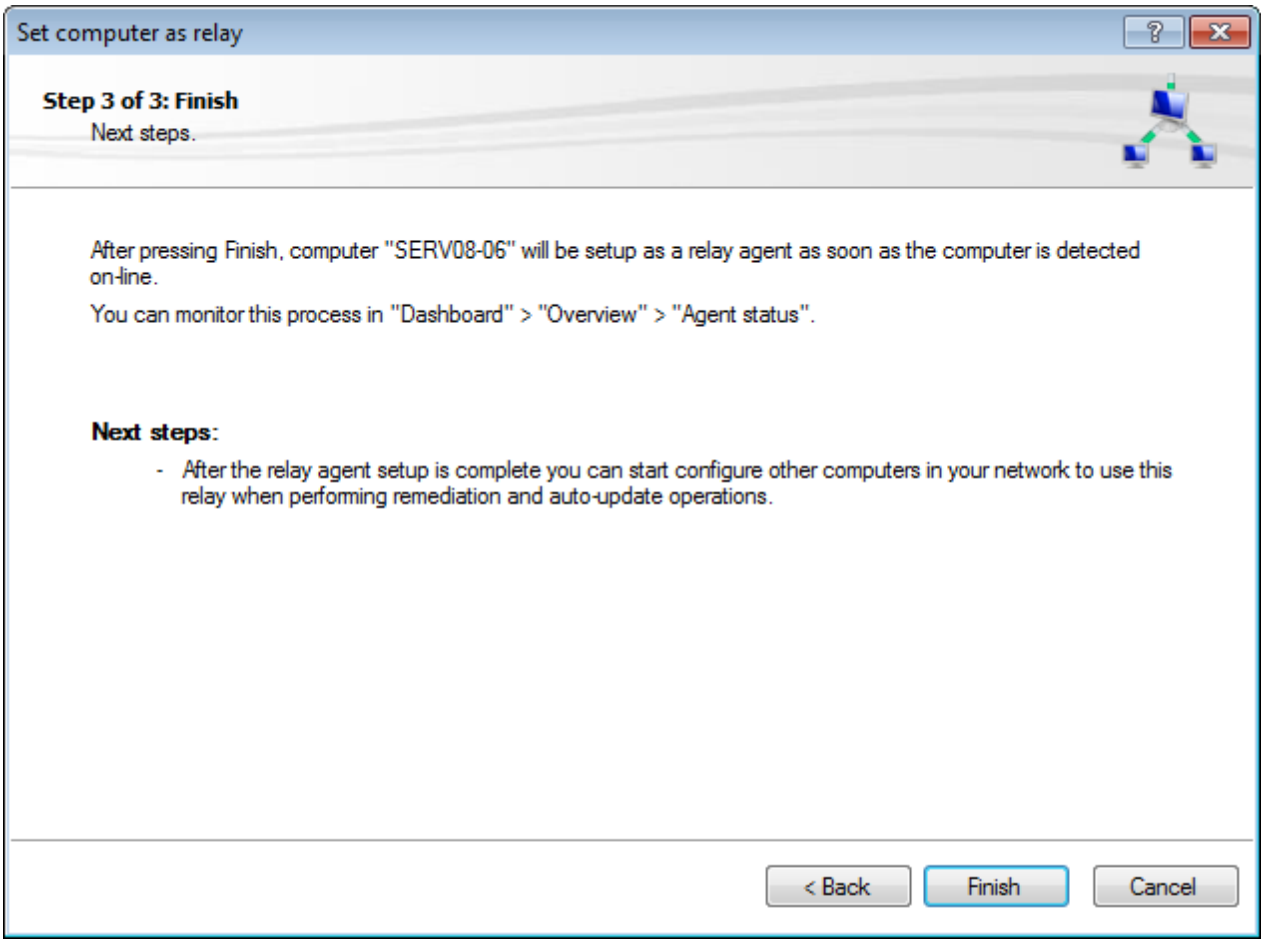

Set computer as relay
Step 2 of 3: Cache location
Choose the caching location on the remote computer.
Choose the location where the relay agent will do the caching:
%AgentData%\RelayCache\
Note: A relay agent requires at least 5 GB of free space to work correctly.
Use %AgentData% as placeholder for agent data folder.
Last known disk drives information:
C: Total space 29.90 GB (Free 22.04 GB)
< Back
Next
Cancel

Screenshot 24: Choose caching directory for the new Relay Agent

6. Choose the caching location for the Relay Agent. The caching directory is used by the relay to store audit and remediation information when auditing remote computers. By default, the **RelayCache** folder is created in `C:\ProgramData\GFI\LanGuard 11\RelayCache`. Click **Next**.

Note

Use the **%AgentData%** placeholder to quickly refer to the Agent's data folder.


Set computer as relay
Step 3 of 3: Finish
Next steps.
After pressing Finish, computer "SERV08-06" will be setup as a relay agent as soon as the computer is detected on-line.
You can monitor this process in "Dashboard" > "Overview" > "Agent status".
Next steps:
- After the relay agent setup is complete you can start configure other computers in your network to use this relay when performing remediation and auto-update operations.
< Back
Finish
Cancel

Screenshot 25: Settings summary step

7. Click **Finish**.

> **Note**
>
> After you click **Finish**, the selected Agent is configured as a Relay Agent. You can monitor this process from **Dashboard > Overview > Agent status**.

4.5.2 Configuring Relay Agent advanced options

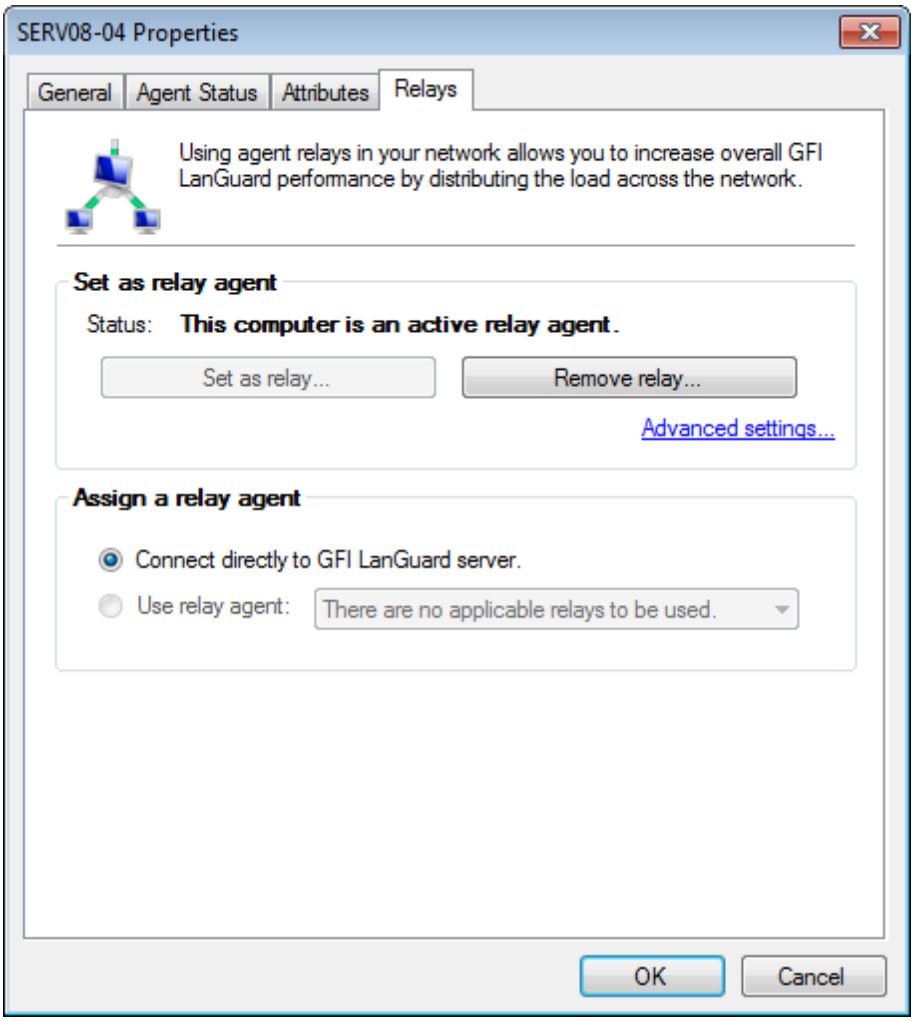
To configure Relay Agent advanced options:

1. Open GFI LanGuard.

2. Click **Configuration** tab **> Agents Management**.

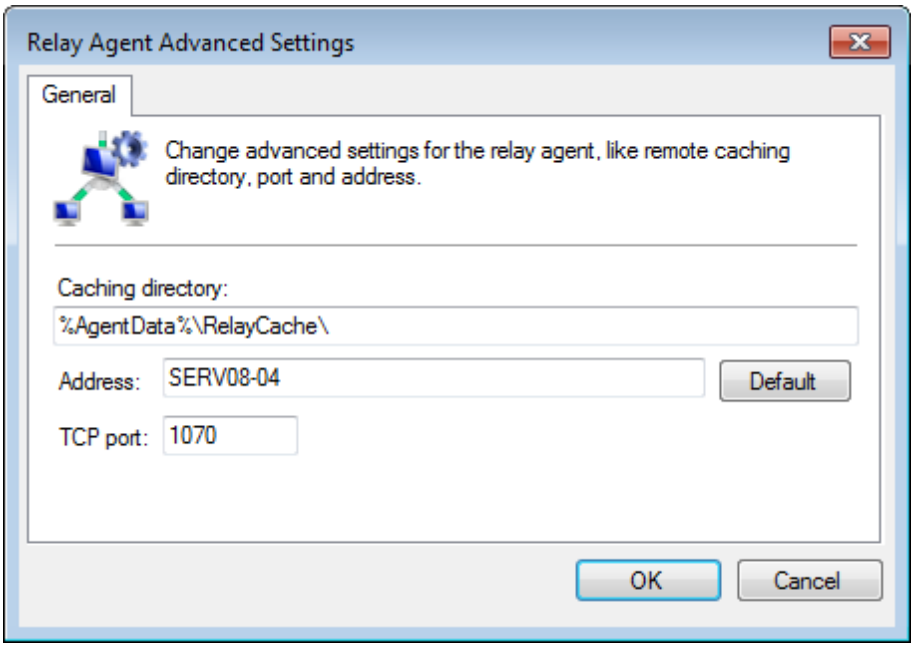
3. Right-click on the Agent you want to configure and select **Properties**. This opens the Agent's **Properties** dialog.

> **Note**
>
> Alternatively, right-click on an computer/group from the computer tree and select **Properties**.


SERV08-04 Properties
General
Agent Status
Attributes
Relays
Using agent relays in your network allows you to increase overall GFI LanGuard performance by distributing the load across the network.
Set as relay agent
Status: This computer is an active relay agent.
Set as relay...
Remove relay...
Advanced settings...
Assign a relay agent
Connect directly to GFI LanGuard server.
Use relay agent:
There are no applicable relays to be used.
OK
Cancel

Screenshot 26: Relay Agent properties - Advanced settings

4. Click **Relays** tab > **Advanced settings...**



Screenshot 27: Relay Agent advances settings dialog

5. From the **Relay Agent Advanced Settings** dialog, configure the options described below:

Table 19: Relay Agent - Advanced options

Option	Description
Caching directory	Location where the relay agent caches information when auditing remote computers.
Address	Displays the computer name that is running the relay agent. Click **Default** to restore the field to its original value.
TCP port	Communication port used by the relay agent to communicate with GFI LanGuard server. Port 1070 is assigned by default and is automatically changed if GFI LanGuard detects that port 1070 is being used by another application.

6. Click **OK**.

4.5.3 Connecting computers to a Relay

To connect a computer to a Relay:

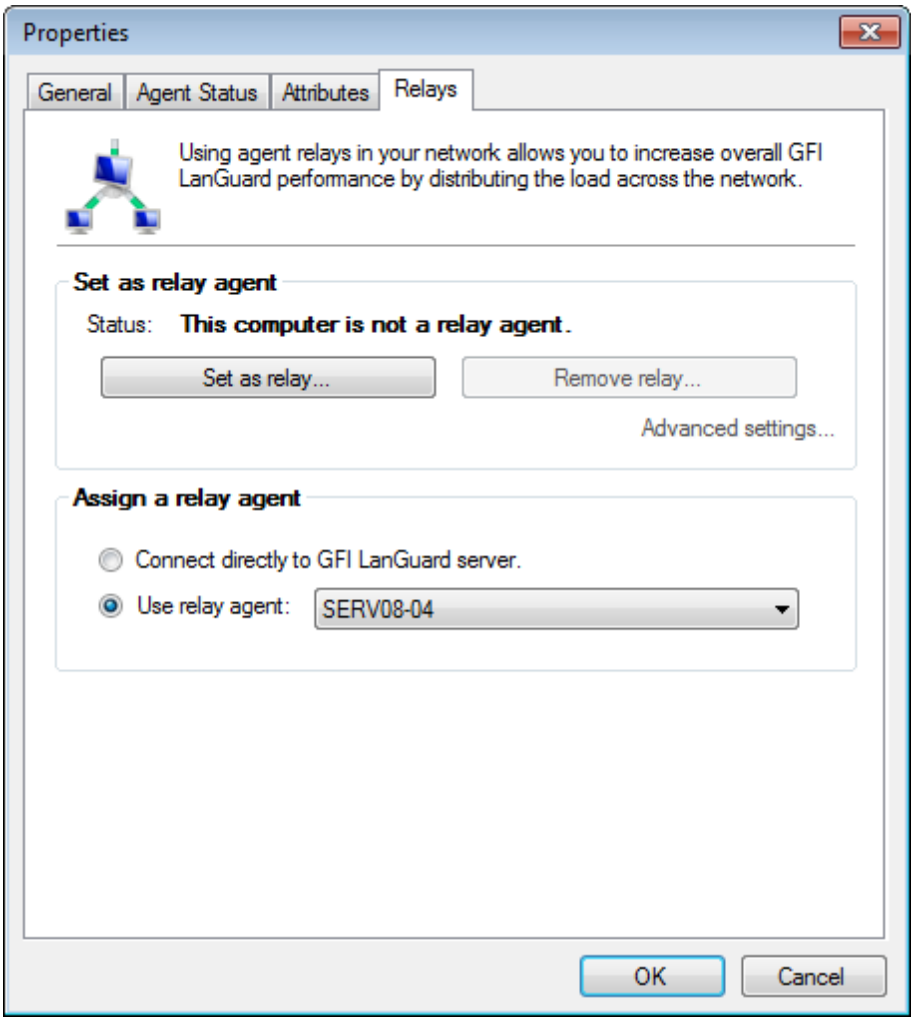
1. Open GFI LanGuard.

2. Click **Configuration** tab > **Agents Management**.

3. Right-click on the Agent you want to configure and select **Properties**. This opens the Agent's **Properties** dialog.

> **Note**
>
> Alternatively, right-click on an computer/group from the computer tree and select **Properties**.

4. Click **Relays** tab.



Screenshot 28: Connecting to a Relay Agent

5. From the **Assign a relay agent** area, select **Use relay agent** and choose the relay from the drop-down menu.

6. Click **OK**.

4.6 Managing Agent groups

The computer tree enables you to configure agent properties of groups of computers. To configure computer group properties:

1. From the computer tree, right-click a group of computers and click **Properties**.

2.(Optional) From **General** tab, specify name, type and authentication method for the selected group.

3. Select **Agent Status** tab, and configure the following options:

Table 20: Agent group status

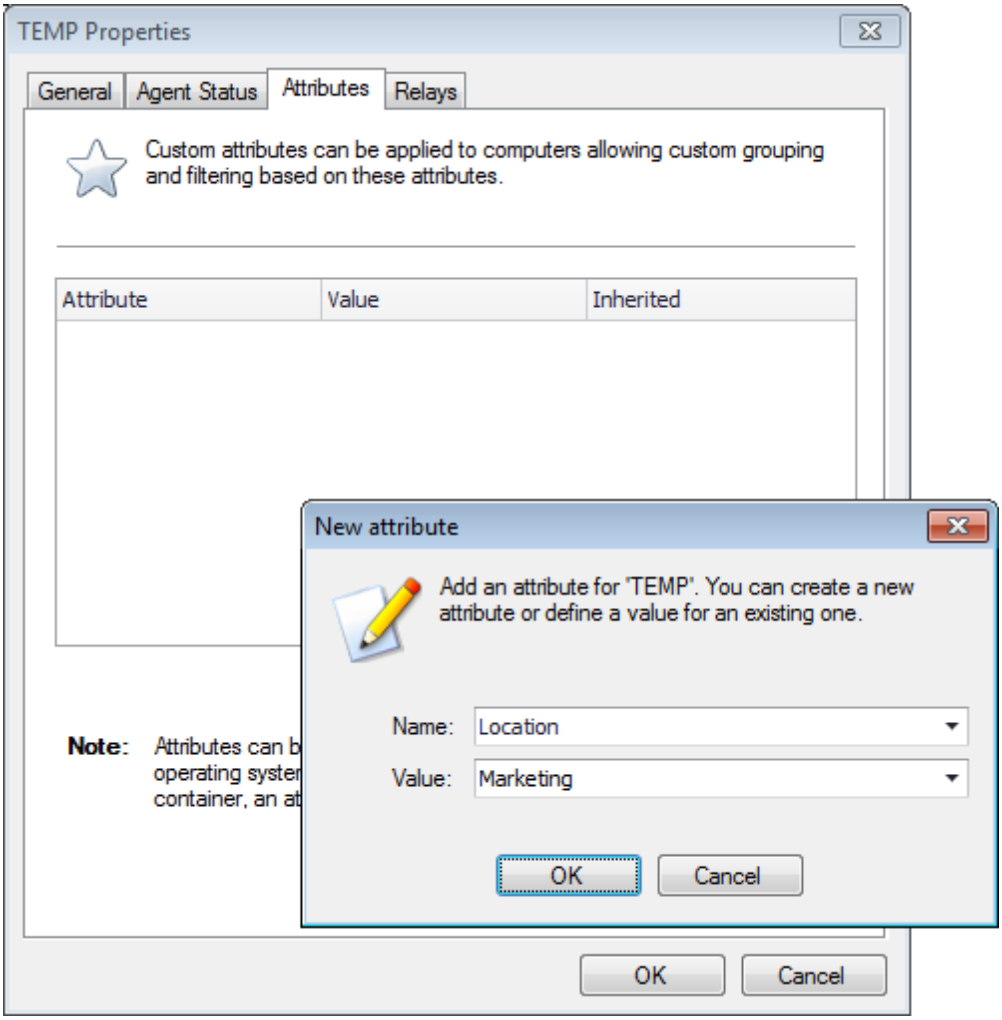
Option	Description
Enable automatic agents deployment	Automatically deploy agents on newly discovered computers.
Remove all agents	Remove all installed agents from this group.
Change scan schedule	Configure the schedule, when GFI LanGuard searches for new computers.
Scanning profile	Configure the audit schedule; when target computers are scanned.
Auto remediation settings	Configure the auto remediation actions to perform on all computers in this group. For more information, refer to Configuring Agent auto-remediation (page 136).

4. Select **Network Discovery** and configure the following options:

Table 21: Agent group network discovery

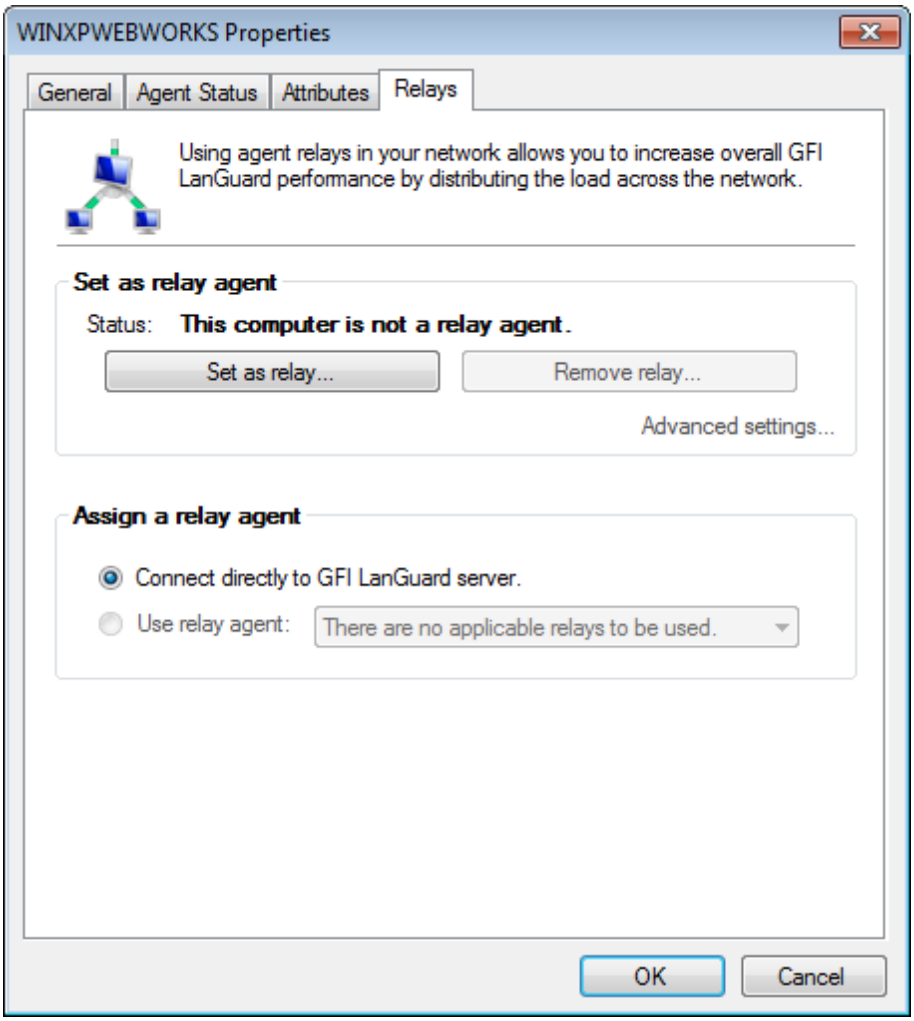
Option	Description
Check automatically for new machines in this group	GFI LanGuard will search for new machines automatically.
Change schedule	Change the schedule when GFI LanGuard searches for new computers.
Run now	Run network discovery.
Scan OU recursively	Recursively, loop through all organization units and enroll computers.

5. Select**Attributes** tab to manage the attributes assigned to the computer selected. Use the **Add**, **Edit** and **Remove** buttons to manage attributes.



Screenshot 29: Agent Attributes

6. Click **Relays** tab to configure agent relays. Relays enable computers other than the one hosting GFI LanGuard to act as GFI LanGuard server. This helps you load-balance traffic directed to that machine and optimize network scanning performance.


WINXPWEBWORKS Properties
General
Agent Status
Attributes
Relays
Using agent relays in your network allows you to increase overall GFI LanGuard performance by distributing the load across the network.
Set as relay agent
Status: This computer is not a relay agent.
Set as relay...
Remove relay...
Advanced settings...
Assign a relay agent
Connect directly to GFI LanGuard server.
Use relay agent:
There are no applicable relays to be used.
OK
Cancel

Screenshot 30: Agent Relays

7. Configure the options described below:

Table 22: Agent relay options

Option	Description
Connect directly to GFI LanGuard server	The selected computer will download product updates and patches from the GFI LanGuard server.
Use relay agent	The selected computer will use a relay agent to download product updates and patches. Select the relay agent to use from the drop down list.

Note

Some options are disabled because they are applicable only for single computers.

8. Click **OK**.

5 Scanning Your Network

This chapter provides you with information about the different scanning profiles that ship with GFI LanGuard, as well as how to trigger immediate or scheduled manual scans. Select the most suitable scanning profile and scanning mode (such as using Agent-less versus Agent-based scans), depending on the availability and location of your scan targets.

Topics in this chapter:

5.1 About Scanning Profiles 64

5.2 Available Scanning Profiles 64

5.3 Manual scans 66

5.4 Enabling security audit policies 69

5.5 Scheduled scans 70

5.6 Agent scheduled scans 80

5.1 About Scanning Profiles

GFI LanGuard enables you to scan your IT infrastructure for particular vulnerabilities using pre-configured sets of checks known as scanning profiles. Scanning profiles enable you to scan your network targets and enumerate only specific information. For example, you may want to use a scanning profile that is set to be used when scanning the computers in your DMZ as opposed to your internal network.

In practice, scanning profiles enable you to focus your vulnerability scanning efforts on to a specific area of your IT infrastructure, such as identifying only missing security updates. The benefit is that you have less scan results data to analyze; tightening up the scope of your investigation and help you quickly locate the information that you require, more easily.

Through multiple scanning profiles, you can perform various network security audits without having to go through a reconfiguration process for every type of security scan required.

5.2 Available Scanning Profiles

GFI LanGuard ships with the default scanning profiles described in the sections below. To create your own custom scanning profiles, refer to Creating a new Scanning Profile. Use the information provided in the following sections to understand what each scanning profile detects on your scan targets:

- Complete/Combination Scans profiles
- Vulnerability Assessment profiles
- Network and Software Audit profiles

5.2.1 Complete/Combination Scans

Table 23: Complete/Combination scanning profiles

Complete/Combination Scans profiles	
Full Vulnerability Assessment	Use this scanning profile to enumerate particular network vulnerabilities such as open TCP/UDP ports commonly exploited by Trojans as well as missing patches and service packs. The list of vulnerabilities enumerated by this profile can be customized through the Vulnerabilities tab. Installed USB devices and applications are not enumerated by this profile. This profile will scan for all vulnerabilities. This includes vulnerabilities which have an associated Microsoft® patch to them and which are considered missing patches.
Full Scan (Active)	Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices connected and more. The vulnerability check timeouts in this profile are specifically preconfigured to suite the network traffic and transmission delays usually associated with LAN environments.
Full Scan (Slow Networks)	Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices connected and more... The vulnerability check timeouts in this profile are specifically preconfigured to suite the network traffic and transmission delays usually associated with WAN environments.

5.2.2 Vulnerability Assessment

Table 24: Vulnerability assessment scanning profiles

Vulnerability Assessment profiles	
Top SANS 20 Vulnerabilities	Use this scanning profile to enumerate all vulnerabilities reported in the SANS top 20 list.
High Security Vulnerabilities	Use this scanning profile to enumerate open TCP/UDP ports and high security vulnerabilities. The list of TCP/UDP ports and high security vulnerabilities that will be enumerated by this profile can be customized through the TCP/UDP Ports tabs and the Vulnerabilities tab respectively.
Last Year's Vulnerabilities	Use this scanning profile to enumerate network vulnerabilities that emerged during the last 12 months.
Only Web	Use this scanning profile to identify web-server specific vulnerabilities. This includes scanning and enumerating open TCP ports that are most commonly used by web-servers such as port 80. Only TCP ports commonly used by web-servers are scanned by this profile. Network auditing operations as well as enumeration of vulnerabilities and missing patches are not performed using this profile.
Missing Patches	Use this scanning profile to enumerate missing patches. The list of missing patches that will be enumerated by this profile can be customized through the Patches tab.
Critical Patches	Use this scanning profile to enumerate only missing patches that are tagged as critical. The list of critical patches that will be enumerated by this profile can be customized through the Patches tab.
Last Month's Patches	Use this scanning profile to enumerate only missing patches that were released last month. The list of missing patches that will be enumerated by this profile can be customized through the Patches tab.
Only Service Packs	Use this scanning profile to enumerate missing service packs. The list of service packs that will be enumerated by this profile can be customized through the Patches tab.
Non-Microsoft® Patches	Use this scanning profile to enumerate missing Third-Party patches, such as Adobe products.
Security Patches	Use this scanning profile to enumerate missing Microsoft® and non-Microsoft® Security Patches on your scan targets.

5.2.3 Network & Software Audit

Table 25: Network & Software Audit

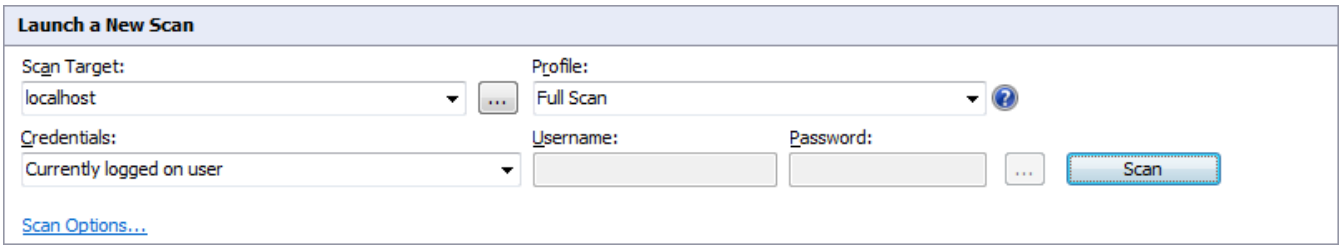
Network & Software Audit profiles	
Trojan Ports	Use this scanning profile to enumerate open TCP/UDP ports that are commonly exploited by known Trojans. The list of TCP/UDP ports to be scanned can be customized through the TCP Ports and UDP Ports tabs respectively. Only the TCP/UDP ports commonly exploited by known Trojans are scanned by this profile. Network auditing operations as well as enumeration of other open TCP/UDP ports and missing patches are not performed by this profile.
Port Scanner	Use this scanning profile to enumerate open TCP/UDP ports including those most commonly exploited by Trojans. The list of ports that will be enumerated by this profile can be customized through the TCP/UDP ports tab.
Software Audit	Use this scanning profile to enumerate all software applications installed on scan targets. This includes security software such as anti-virus and anti-spyware.
Full TCP & UDP Scan	Use this scanning profile to audit your network and enumerate all open TCP and UDP ports.
Only SNMP	Use this scanning profile to perform network discovery and retrieve information regarding hardware devices (routers, switches, printers, etc.) that have SNMP enabled. This enables you to monitor network-attached devices for conditions that require administrative attention.
Ping Them All	Use this scanning profile to audit your network and enumerate all computers that are currently connected and running.
Share Finder	Use this scanning profile to audit your network and enumerate all open shares either hidden or visible. No vulnerability checks are performed by this profile.
Uptimes	Use this scanning profile to audit your network and identify how long each computer has been running since the last reboot.
Disks Space Usage	Use this scanning profile to audit your network and retrieve system information on available storage space.
System Information	Use this scanning profile to retrieve system information such as operating system details, wireless/virtual/physical network devices connected, USB devices connected, installed applications and more.
Hardware Audit	Use this scanning profile to audit your network and enumerate all hardware devices currently connected to your network computers.
Network Discovery	Use this scanning profile to enumerate any IP enabled device connected to your network.

5.3 Manual scans

Manual scan is the process of performing audits on target computers without using agents. To perform a manual scan on a specific computer:

1. Launch GFI LanGuard.

2. From the **Home** tab click **Launch a Scan**. Alternatively, click the **Scan** tab.



Screenshot 31: Manual scan settings

3. From the **Scan Target** drop-down menu, select the target computer or group of computers to scan using the following options:

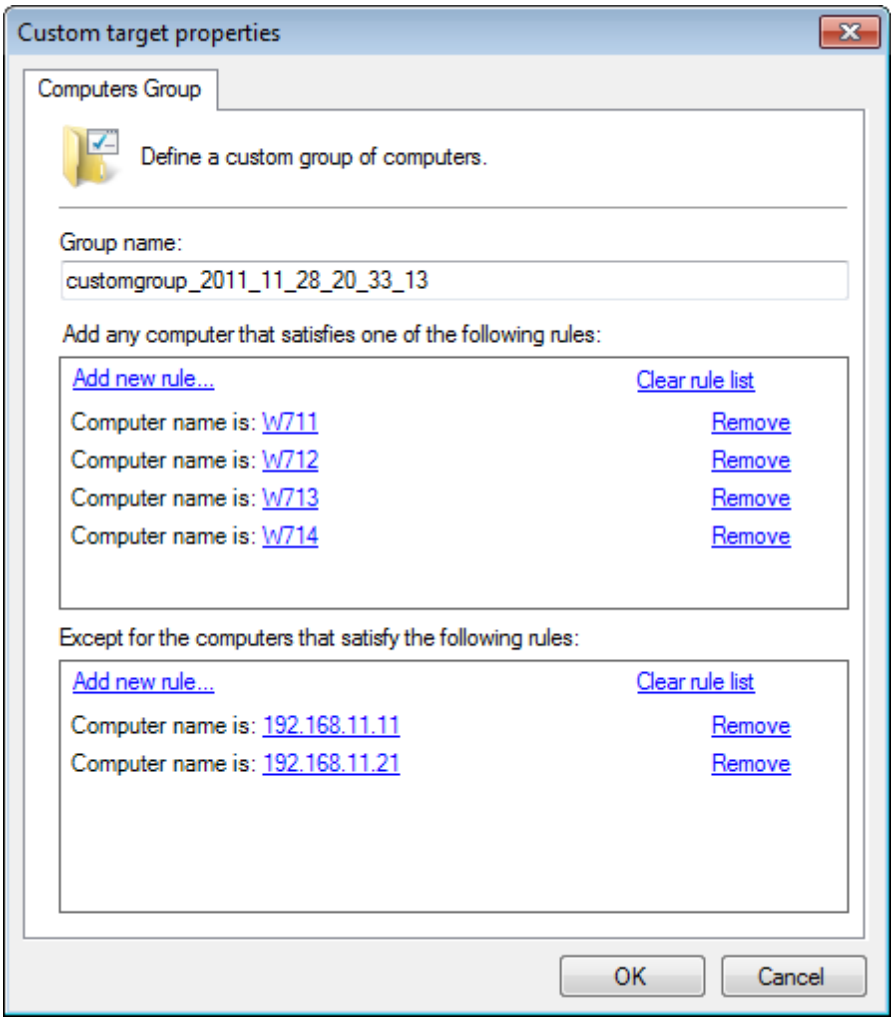
Table 26: Target options when auditing

Option	Description
Localhost	Audit the local host where GFI LanGuard is installed.
Domain: primary domain	Audit the entire domain / workgroup of the computer / server where GFI LanGuard is installed.

Note

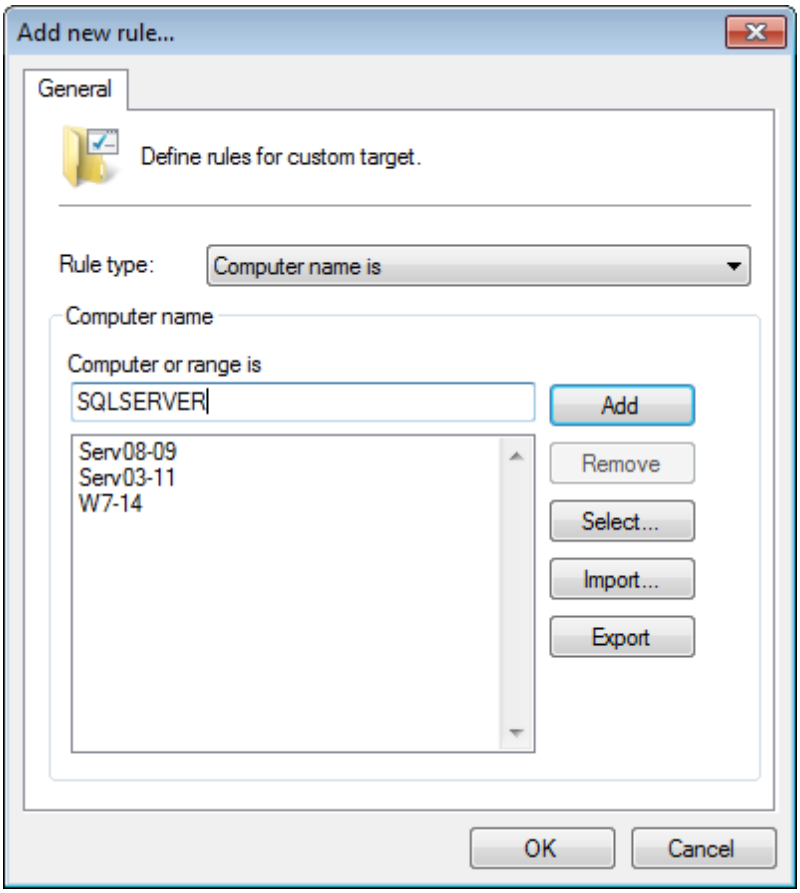
Optionally, from the computer tree, right-click a computer/computer group and select **Scan > Custom Scan**.

4. Click the browse button (**...**) to define custom rules for adding scan targets.



Screenshot 32: Custom target properties

5. From the **Custom target properties** dialog, click **Add new rule** links to create a custom rule for computers you want to scan or exclude from scanning.



Screenshot 33: Add new rule...

6. From the **Add new rule** dialog, select the **Rule type** described below to add computers:

Table 27: Custom target properties

Rule type	Description
Computer name is	Search and add computers by name. Key-in a valid computer name and click **Add** for each computer. Click **OK** to apply changes.
Computers file list is	Search and add computers from a text file. Click the browse button and locate the text file. Click **OK** to apply changes. **Note** When submitting a list of target computers from file, ensure that the file contains only one target computer name per line.
Domain name is	Search and add computers that are members of a domain. Select the domains from the list and click **OK**.
IP address is	Search and add computers by IP address. Select **This computer** to add the local host or **Scan another computer** to add a remote computer. Key-in the IP address if required and click **OK**.
IP address range is	Search and add computers within an IP range. Select **Scan an IP address range** and key in the IP range or select CIDR subnet and key-in the range using CIDR notation. **Note** The Classless Inter-Domain Routing (CIDR) provides an alternative way of specifying an IP address range. The notation is as follows: `<Base address> / <IP network prefix>`. Example: 192.168.0.0/16
Organization unit is	Search and add computers within an organizational unit. Click **Select** and from the list select the Organizational units. Click **OK**.

7. Once the rules are added, click **OK** to close the **Add new rule dialog**. Click **OK** to close the **Custom target properties** dialog and return to the scan settings.

8. From the **Profile** drop-down menu, select the scan profile that you want GFI LanGuard to action during the scan. For more information, refer to Available Scanning Profiles (page 64).

9. From the **Credentials** drop-down menu, select the log-on method used by GFI LanGuard to log onto the scan targets. The table below describes the available options:

Table 28: Logon and audit options

Option	Description
Currently logged on user	Use the current logged on user credentials when logging on scan targets.
Alternative credentials	Use custom credentials. Key-in the user name and password to use.
A null session	Log onto scan targets using a null session. The user will log onto the target machine as an anonymous user.
A private key file	Log onto UNIX machines using SSH. A user name and password is required.

> **Note**
>
> The credentials provided need to have administrator privileges in order for GFI LanGuard to log-on to the target computers and carry out the network audit.

10. (Optional) Click **Scan Options** and configure the options described below:

Table 29: Scan options

Option	Description
Use per computer credentials when available	Logon target machines using the credentials specified in the Dashboard
Remember credentials	Use the configured credentials as default when performing an audit.
Wake up offline computers	GFI LanGuard attempts to power on offline computers using Wake-on-LAN. For more information, refer to Configuring Wake-on-LAN on scan targets (page 130).
Shut down computers after scan	Shut down when a scan is complete.

11. Click **Scan** to start auditing the selected targets.

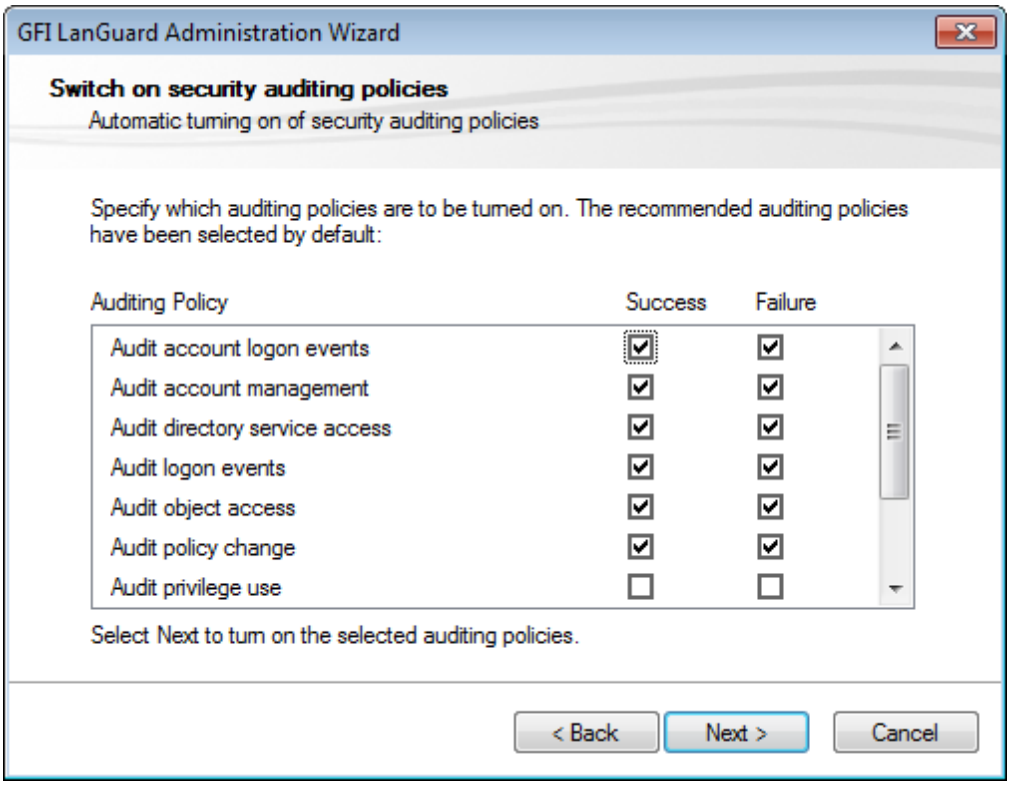
5.4 Enabling security audit policies

An important part of any security plan is the ability to monitor and audit events on your network. These event logs are frequently referenced to identify security holes or breaches. Identifying attempts and preventing them from becoming successful breaches of your system security is critical. In Windows, you can use **Group Policies** to set up an audit policy that can track user activities or system events in specific logs.

To keep track of your system auditing policy, GFI LanGuard collects the security audit policy settings from target computers and includes them in the scan result. To access more information on the result click on **Security Audit Policy** sub-node.

Apart from gaining knowledge on the current audit policy settings, you can also use GFI LanGuard to access and modify the audit policy settings of your target computers. To achieve this:

1. After scanning a remote computer, from the **Scan Results Overview** panel, right-click on the respective target computer and select **Enable auditing on** > **This computer/Selected computers/All computers**.


GFI LanGuard Administration Wizard
Switch on security auditing policies
Automatic turning on of security auditing policies
Specify which auditing policies are to be turned on. The recommended auditing policies have been selected by default:
Auditing Policy
Success
Failure
Audit account logon events
Audit account management
Audit directory service access
Audit logon events
Audit object access
Audit policy change
Audit privilege use
Select Next to turn on the selected auditing policies.
< Back
Next >
Cancel

Screenshot 34: The audit policy administration wizard

2. Select/unselect auditing policies accordingly, and click **Next** to deploy the audit policy configuration settings, on the target computer(s).

3. At this stage, a dialog will show whether the deployment of audit policy settings was successful or not. To proceed to the next stage click **Next**. Click **Back** to re-deploy settings on failed computers.

4. Click **Finish** to finalize configuration. Restart a scan to update results.

5.5 Scheduled scans

A scheduled scan is a network audit that is scheduled to run automatically on a specific date/time and at a specific frequency. Scheduled scans can be set to execute once or periodically. Scheduled scan status is monitored using the **Activity Monitor** tab > **Security Scans**.

GFI recommends scheduled scans:

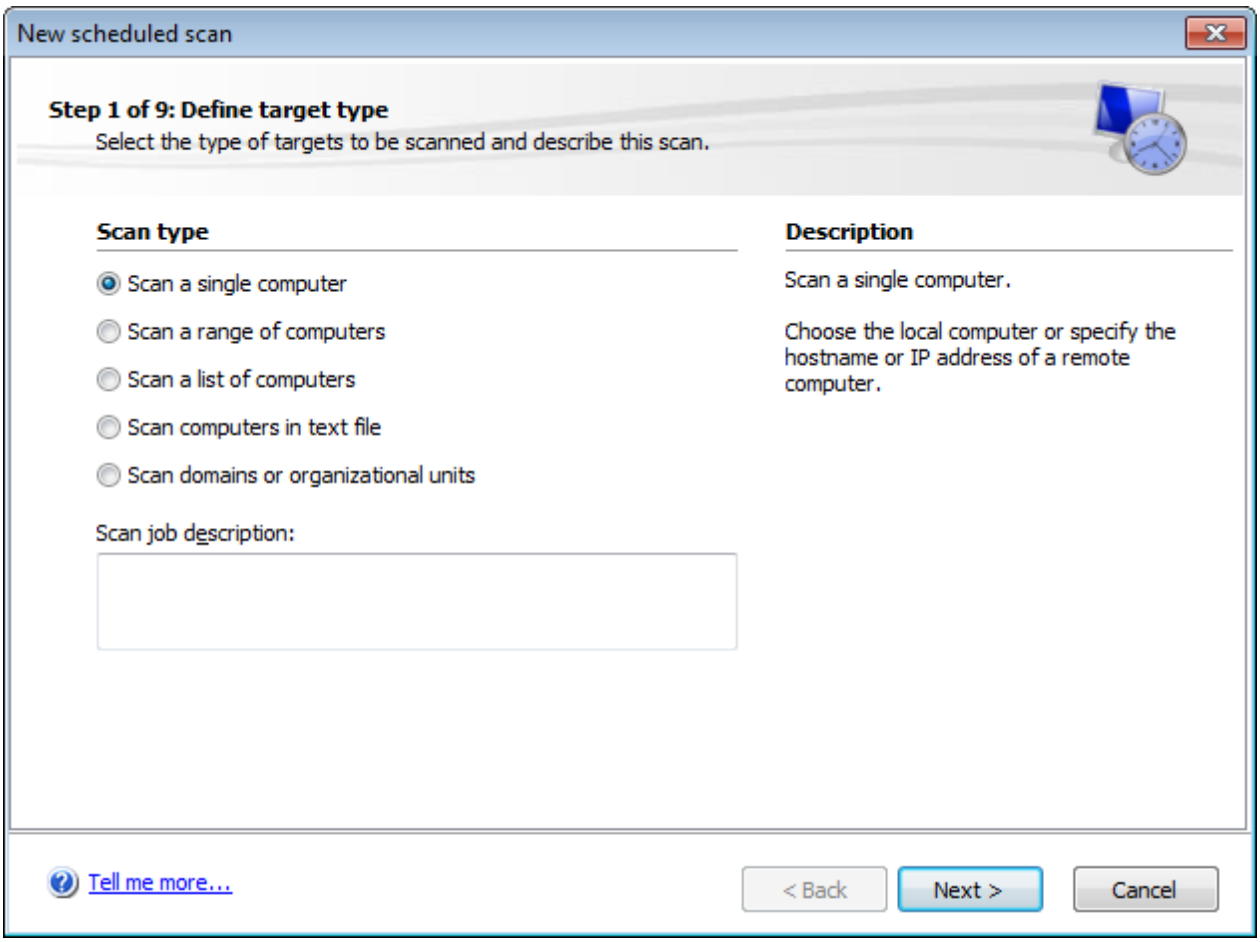
- When GFI LanGuard Agents are not deployed on the target computers
- To automatically perform periodical/regular network vulnerability scans using same scanning profiles and parameters
- To automatically trigger scans after office hours and generate alerts and auto-distribution of scan results via email
- To automatically trigger auto-remediation options, (Example: Auto-download and deploy missing updates).

The following sections contain information to guide you in configuring and executing scheduled scans:

- Creating a scheduled scan
- Editing scheduled scan settings
- Configuring scheduled scan properties

5.5.1 Creating a scheduled scan

1. Launch GFI LanGuard.
2. Click **Configuration** tab > **Scheduled Scans**.
3. From **Common Tasks**, select **New scheduled scan**.


New scheduled scan
Step 1 of 9: Define target type
Select the type of targets to be scanned and describe this scan.
Scan type
Scan a single computer
Scan a range of computers
Scan a list of computers
Scan computers in text file
Scan domains or organizational units
Scan job description:
Description
Scan a single computer.
Choose the local computer or specify the hostname or IP address of a remote computer.
Tell me more...
< Back
Next >
Cancel

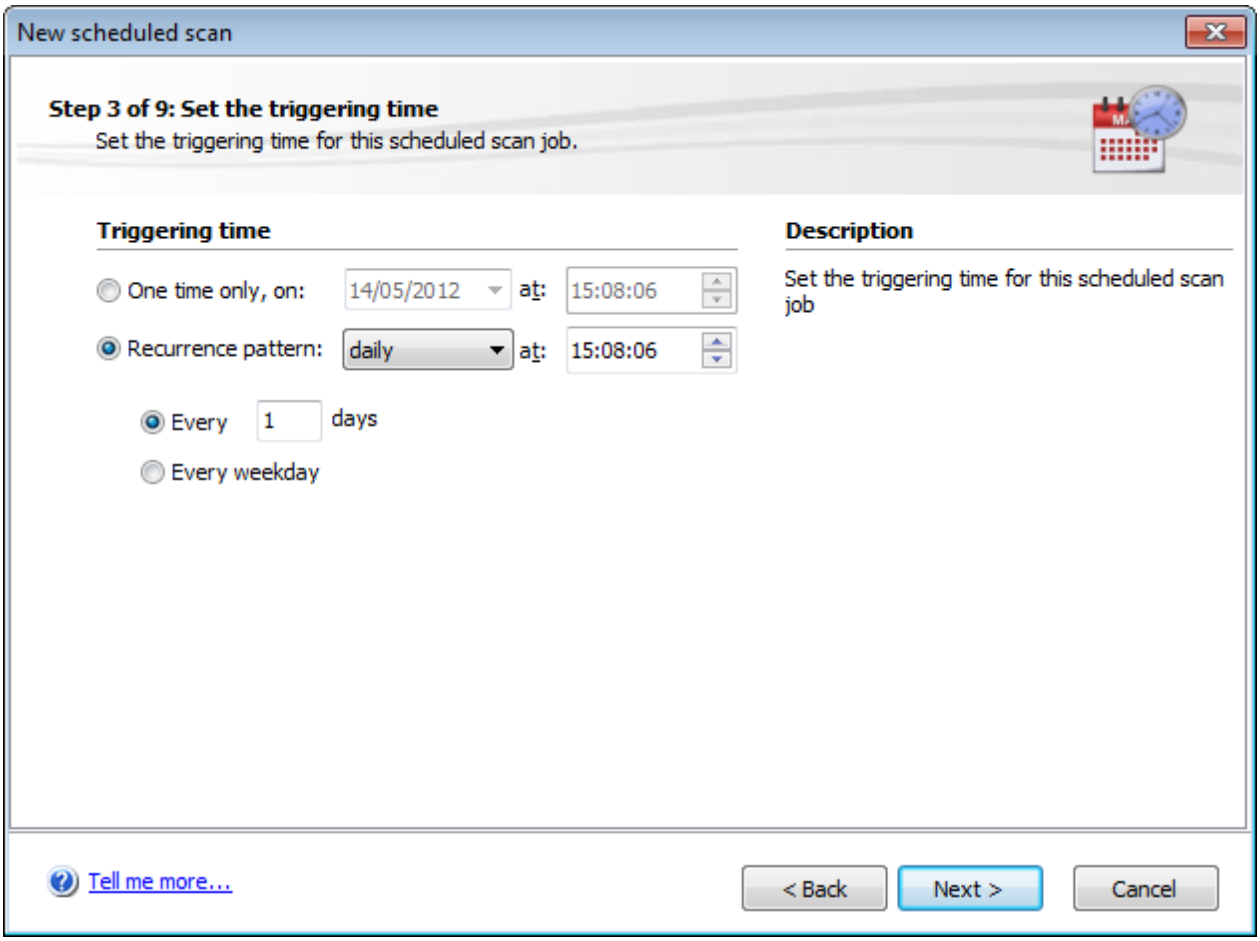
Screenshot 35: New Scheduled Scan dialog

4. Select one of the options described below and click **Next**.

Table 30: New scheduled scan type

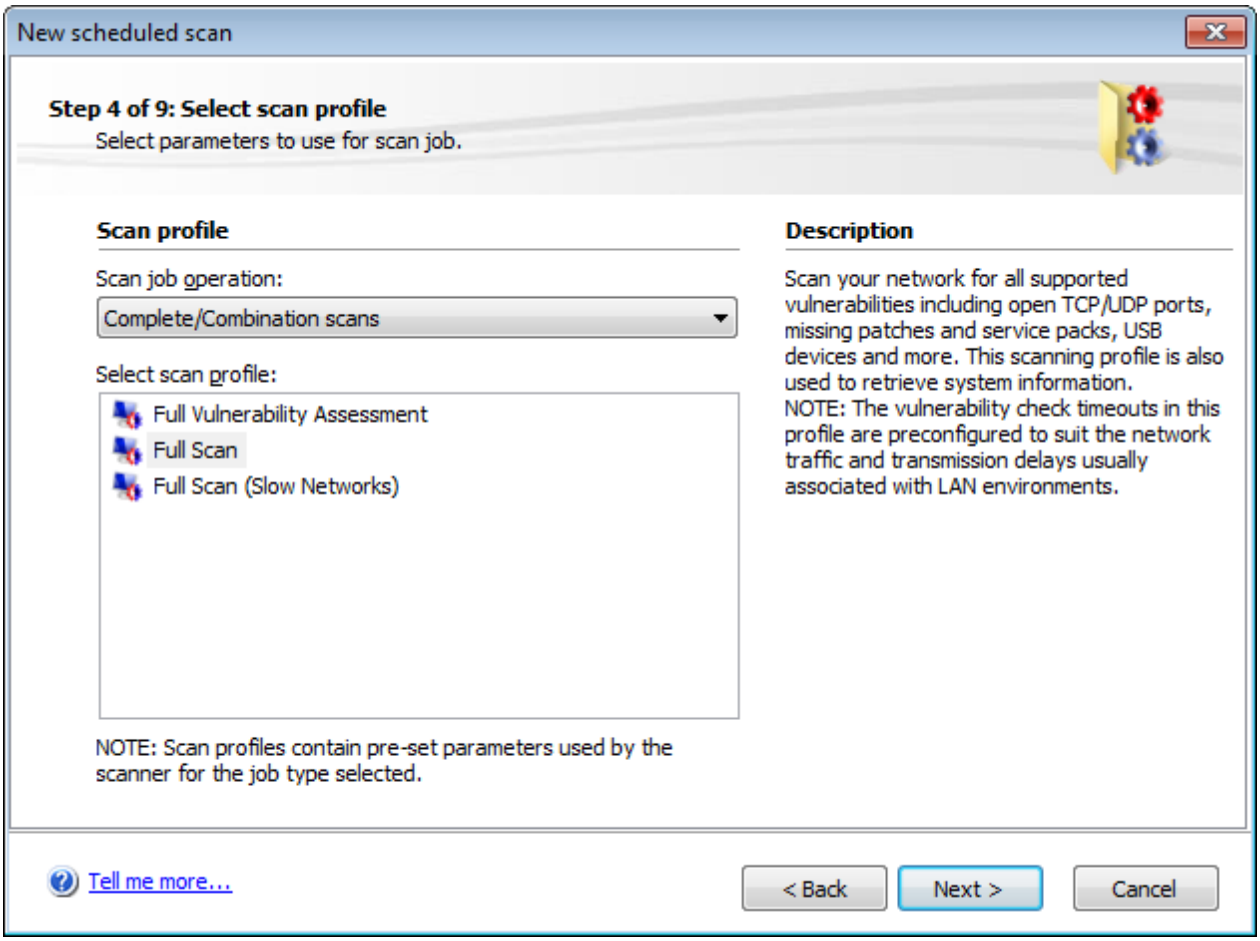
Option	Description
Scan a single computer	Scan local host or one specific computer.
Scan a range of computers	Scan a number of computers defined through an IP range.
Scan a list of computers	Manually create a list of targets, import targets from file or select targets from network list.
Scan computers in text file	Scan targets enumerated in a specific text file.
Scan a domains or organizational units	Scan all targets connected to a specified domain/organizational unit.

5. Depending on the option selected in the previous step, specify the respective target computer(s) details and click **Next**.



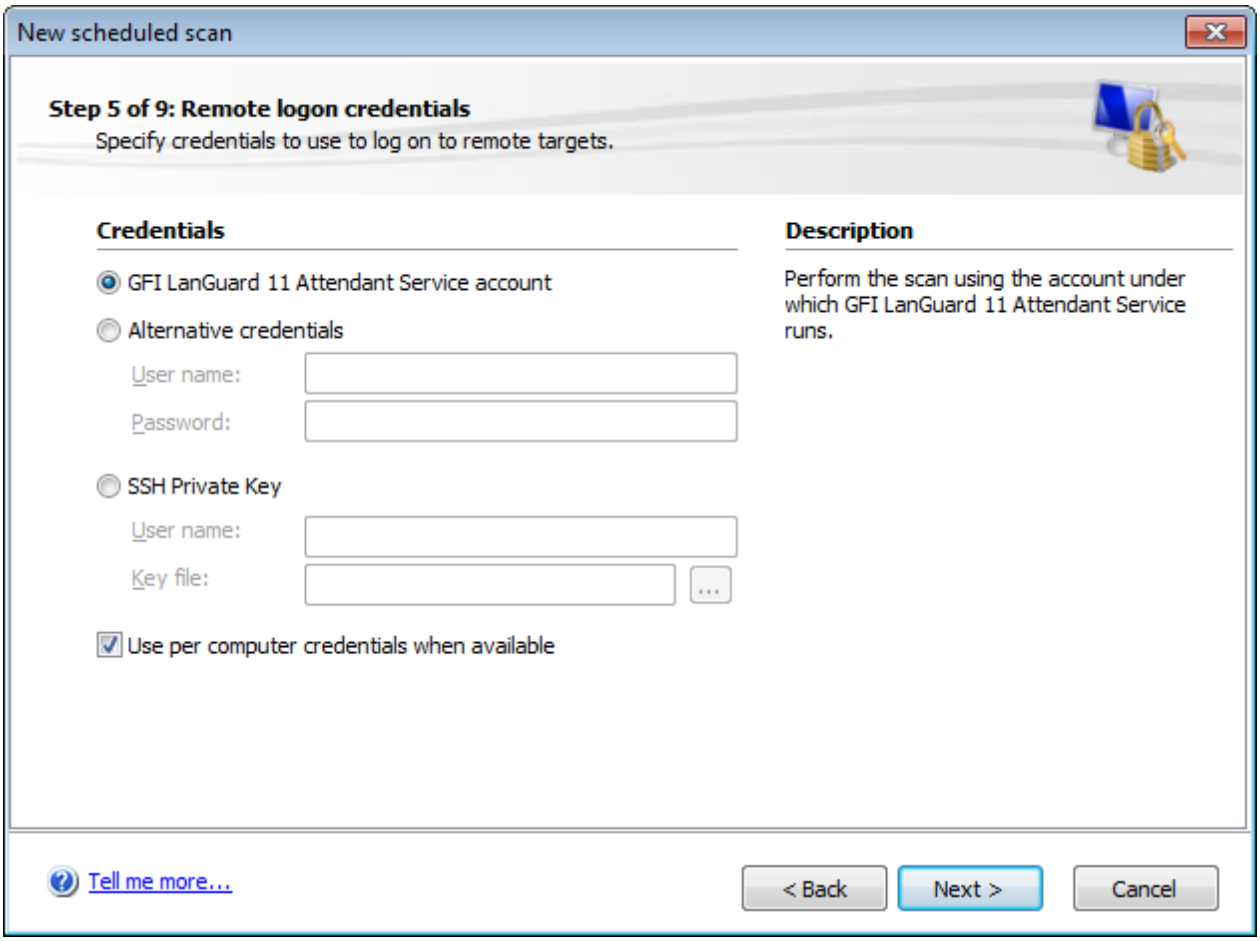
Screenshot 36: Scheduled scan frequency

6. Specify date/time/frequency of the new scheduled scan and click **Next**.


New scheduled scan
Step 4 of 9: Select scan profile
Select parameters to use for scan job.
Scan profile
Scan job operation:
Complete/Combination scans
Select scan profile:
Full Vulnerability Assessment
Full Scan
Full Scan (Slow Networks)
NOTE: Scan profiles contain pre-set parameters used by the scanner for the job type selected.
Description
Scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices and more. This scanning profile is also used to retrieve system information.
NOTE: The vulnerability check timeouts in this profile are preconfigured to suit the network traffic and transmission delays usually associated with LAN environments.
Tell me more...
< Back
Next >
Cancel

Screenshot 37: Select scanning profile

7. From the **Scan job operation** drop-down menu, select the scanning profile to be used during the scan and click **Next**. For more information, refer to Available Scanning Profiles (page 64).

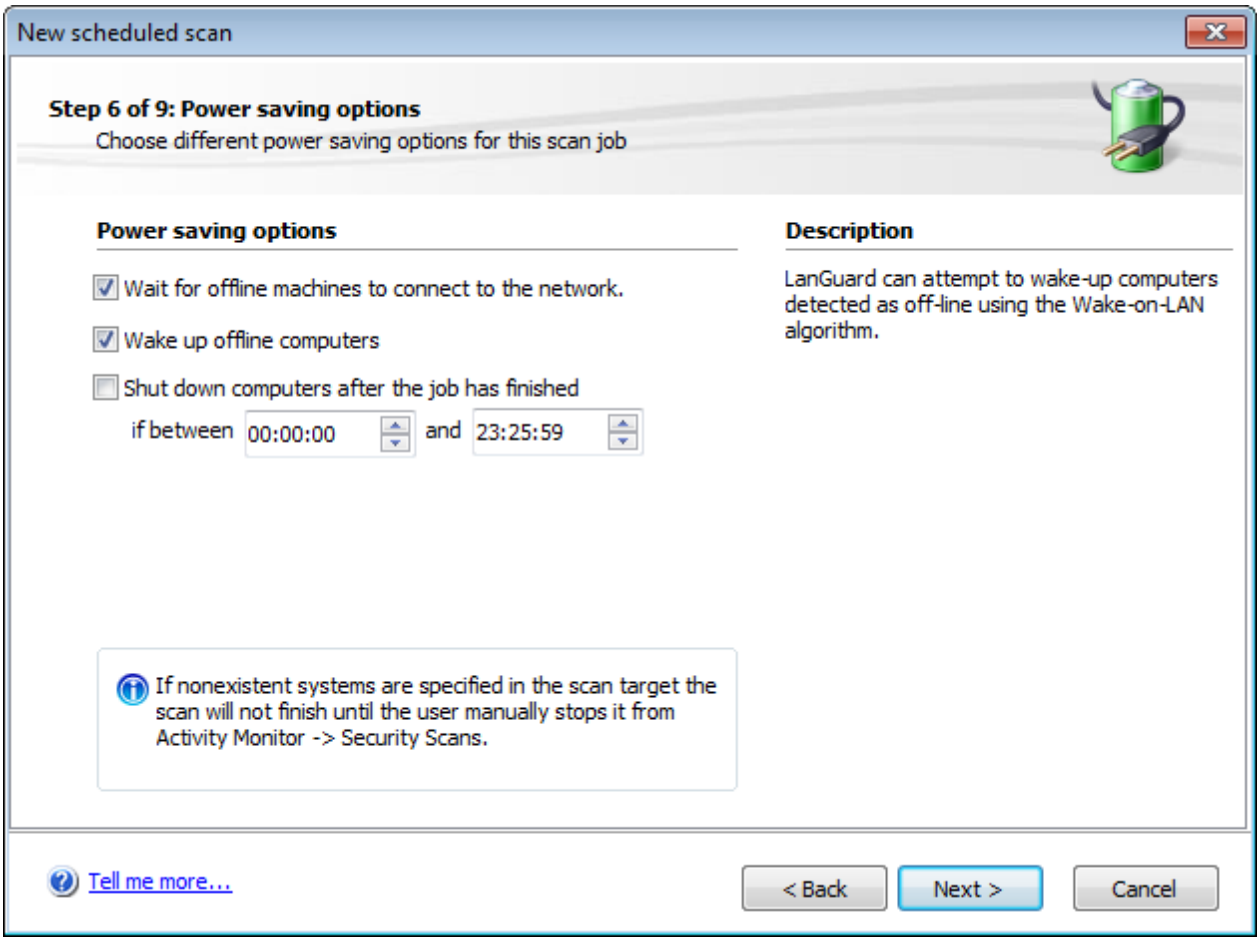


Screenshot 38: Remote logon credentials

8. (Optional) Specify **Remote logon credentials** and click **Next**. Remote logon credentials can be either one of the following:

Table 31: Remote logon credentials

Option	Description
GFI LanGuard 11 Attendant Service account	Performs the scan using the credentials specified while installing GFI LanGuard 2011.
Alternative credentials	Specify alternate credentials to connect to the scan computers. **Note** Ensure the supplied credentials have administrative privileges.
SSH Private Key	Key in a username and select the key file used to logon to UNIX/LINUX based systems.
Use per computer credentials when available	Use predefined credentials for the scan being configured.

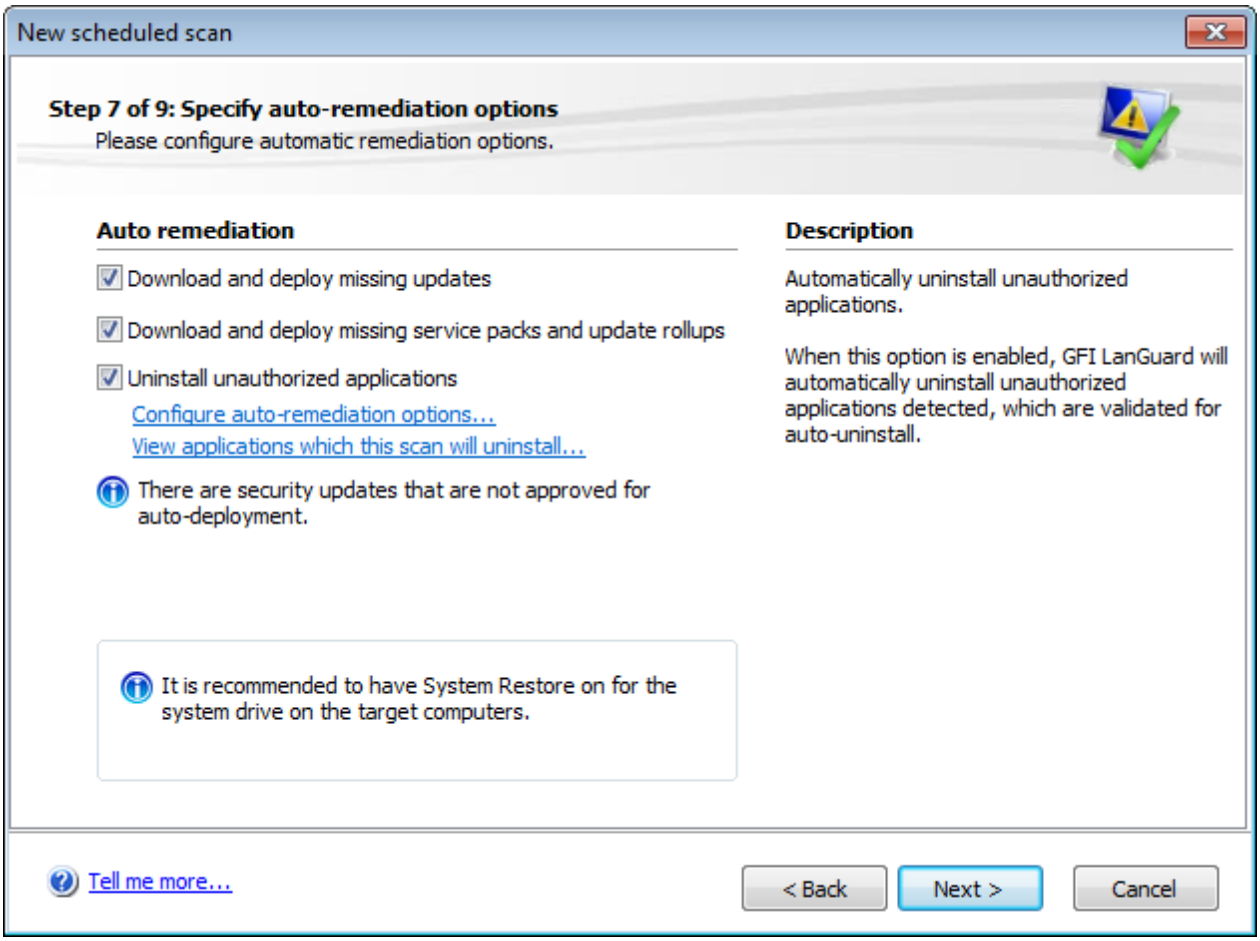

New scheduled scan
Step 6 of 9: Power saving options
Choose different power saving options for this scan job
Power saving options
Wait for offline machines to connect to the network.
Wake up offline computers
Shut down computers after the job has finished
if between 00:00:00 and 23:25:59
Description
LanGuard can attempt to wake-up computers detected as off-line using the Wake-on-LAN algorithm.
If nonexistent systems are specified in the scan target the scan will not finish until the user manually stops it from Activity Monitor -> Security Scans.
Tell me more...
< Back
Next >
Cancel

Screenshot 39: Scheduled scan reporting options

9. From the **Power saving** options, configure the following options:

Table 32: Power saving options

Option	Description
Wait for offline machines to connect to network	Shut down computers after the job has finished
Attempt to wake up off-line computers	GFI LanGuard attempts to power on offline machines using Wake-on-LAN. For more information, refer to Configuring Wake-on-LAN on scan targets (page 130).
Shut down computers after the job has finished	After a computer has been scanned or an auto-remediation job has been done, GFI LanGuard attempts to shut down the computer if the time is in the specified timeframe. **Note** If shut down options are defined in Auto-remediation options, the power saving options are ignored.

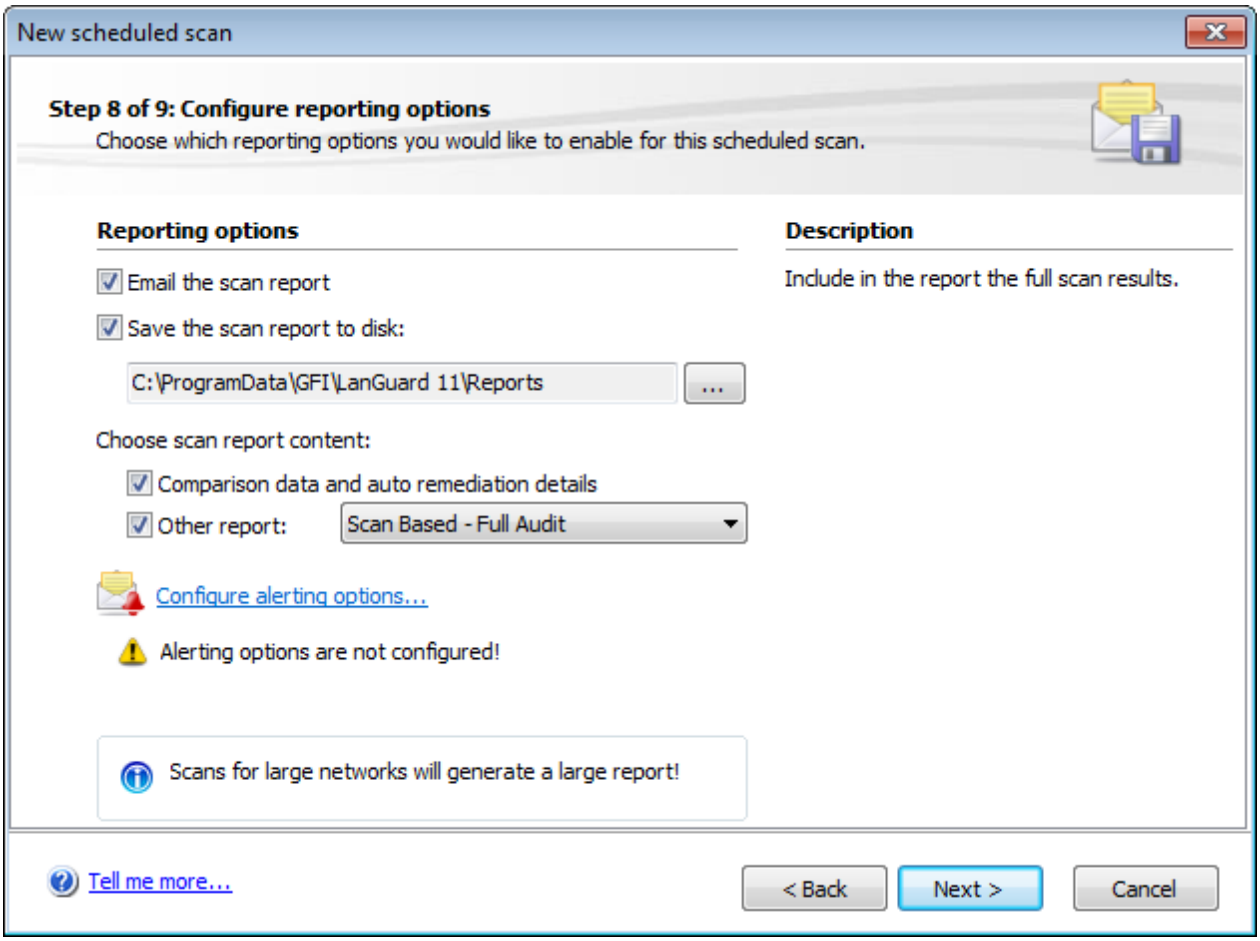

New scheduled scan
Step 7 of 9: Specify auto-remediation options
Please configure automatic remediation options.
Auto remediation
Download and deploy missing updates
Download and deploy missing service packs and update rollups
Uninstall unauthorized applications
Configure auto-remediation options...
View applications which this scan will uninstall...
There are security updates that are not approved for auto-deployment.
It is recommended to have System Restore on for the system drive on the target computers.
Description
Automatically uninstall unauthorized applications.
When this option is enabled, GFI LanGuard will automatically uninstall unauthorized applications detected, which are validated for auto-uninstall.
Tell me more...
< Back
Next >
Cancel

Screenshot 40: Scheduled scan auto-remediation options

10. From the auto-remediation dialog, select the required options and click **Next**. The table below describes the list of available options:

Table 33: Auto-remediation options

Option	Description
Download and deploy missing updates	Automatically download and deploy missing patches on target machines.
Download and deploy missing service packs and update rollups	Automatically download and deploy missing service packs on target machines.
Uninstall unauthorized applications	If this option is selected all applications validated as unauthorized, will be uninstalled from the scanned computer (unauthorized applications are defined in Application Inventory). For more information, refer to Configuring unauthorized applications auto-uninstall (page 121).
Configure auto-remediation	Automatically remove unauthorized applications from target machines. Unauthorized applications are defined in the Application Inventory). For more information, refer to Configuring unauthorized applications auto-uninstall (page 121).
View applications which this scan will uninstall	Click the link to launch the applications which will be uninstalled dialog. This will list all the applications that will be uninstalled when the scheduled scan is finished.

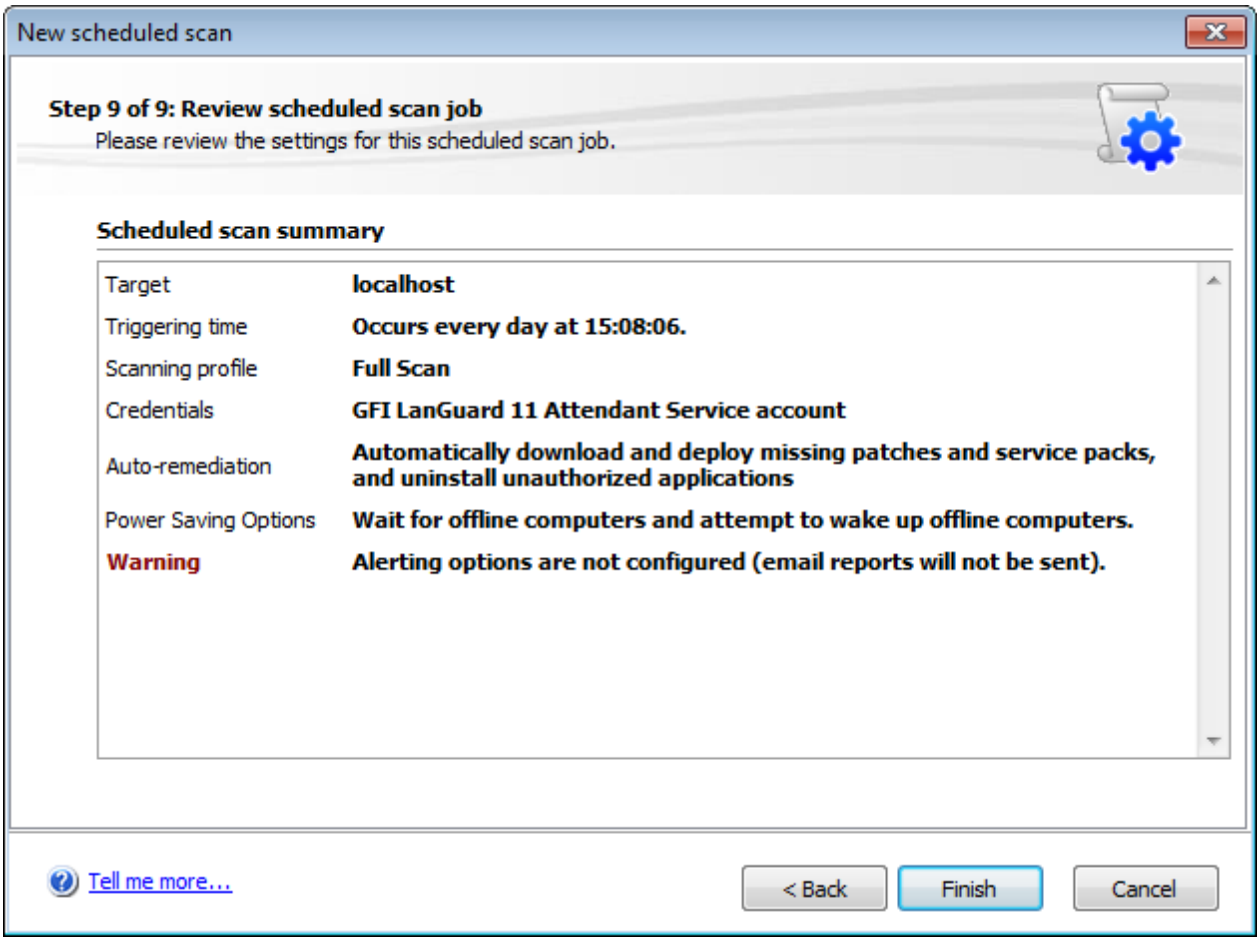

New scheduled scan
Step 8 of 9: Configure reporting options
Choose which reporting options you would like to enable for this scheduled scan.
Reporting options
Email the scan report
Save the scan report to disk:
C:\ProgramData\GFI\LanGuard 11\Reports
...
Choose scan report content:
Comparison data and auto remediation details
Other report:
Scan Based - Full Audit
Configure alerting options...
Alerting options are not configured!
Scans for large networks will generate a large report!
Description
Include in the report the full scan results.
Tell me more...
< Back
Next >
Cancel

Screenshot 41: Scheduled scan reporting options

11. (Optional) Configure **Reporting options** as described below:

Table 34: Reporting options

Option	Description
Email the scan report	Send a report by email at the end of each scheduled scan.
Save the scan report to disk	Save a report to disk at the end of each scheduled scan
Comparison data and auto remediation details	Include details of auto remediation actions performed and result comparison with previous security scans. **Note** Comparison is done between scans with same scan target(s) and scanning profile.
Full scan results data	Include full scan result details.
Configure alerting options	(Optional) Click Configure alerting options... to specify sender/recipient details. For more information, refer to Configuring Alerting Options (page 177).
Override general alerting options, and send email to	(Optional) Send a report by email to specific email address. GFI LanGuard alerting options are overridden.


New scheduled scan
Step 9 of 9: Review scheduled scan job
Please review the settings for this scheduled scan job.
Scheduled scan summary
Target
localhost
Triggering time
Occurs every day at 15:08:06.
Scanning profile
Full Scan
Credentials
GFI LanGuard 11 Attendant Service account
Auto-remediation
Automatically download and deploy missing patches and service packs, and uninstall unauthorized applications
Power Saving Options
Wait for offline computers and attempt to wake up offline computers.
Warning
Alerting options are not configured (email reports will not be sent).
Tell me more...
< Back
Finish
Cancel

Screenshot 42: Scheduled scan reporting options

12. Review the scan settings summary and click **Finish**.

Note

By default, all new scheduled scans are disabled. To enable, select **Configuration** tab > **Scheduled Scans** and click on the button.

Note

Confirm that the new scheduled scans are successfully set by clicking on **Activity Monitor** tab > **Security Scans**. New scheduled scans are listed in the queue.

5.5.2 Editing scheduled scan settings

Scan schedules can be reviewed, edited, or deleted from **Configuration** tab > **Scheduled Scans** node. All scans are listed in the review page together with the relevant information. Use the scheduled scan toolbar to perform the actions described below:

Table 35: Options to manage scanning profiles

Options	
	Add new scan Display the New scheduled scan wizard and create a new scheduled scan.
	Delete Use this button to delete the selected scheduled scan.
	Properties Review and edit the properties of the selected scan.
	Enable/Disable Toggle the status of the selected scan between enabled and disabled. This enables you to activate/suspend a scanning schedule without deleting the scheduled scan.
	Scan now Trigger the selected scheduled scan. This button overrides the scheduled scan date/time settings and executes an immediate scan.

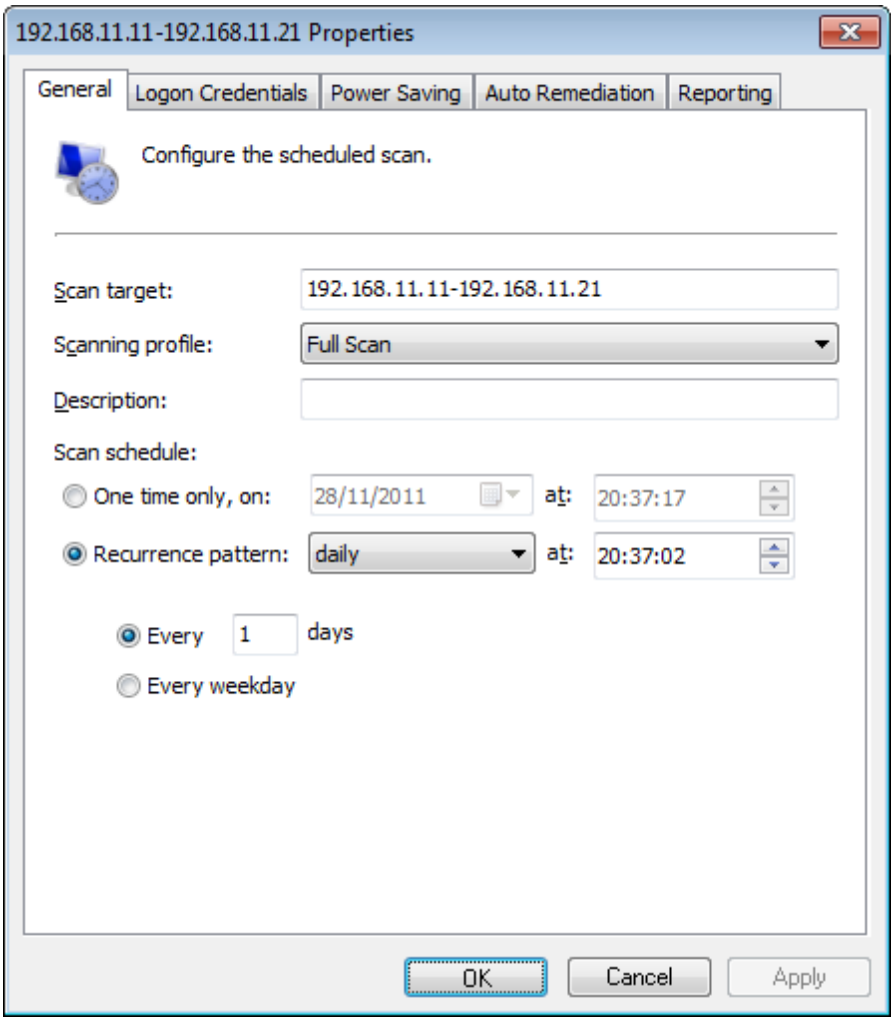
5.5.3 Configuring scheduled scan properties

The scheduled scan properties page enables you to configure all the parameters of the scheduled scans.

To use the scheduled scan properties tab:

1. Go to **Configuration** tab > **Scheduled Scans**.

2. Select the scheduled scan and click the **Scheduled Scan Properties**.



Screenshot 43: Scheduled Scan properties

Table 36: Schedule scan properties

Tab	Description
General	Make changes to scan target setting, type of scanning profile and scan frequency.
Logon Credentials	Specify logon credentials used when scanning the specified target.
Power Saving	Configure power saving options. This dialog enables you to configure the scan to wait for offline machines to connect to the network, attempt to wake up offline machines and shut down machines when the scan is completed.
Auto-remediation	Configure the remediation options applicable to the scan being configured. This includes downloading and installing missing patches and service packs and unauthorized software un-installation.
Reporting	Configure reporting options used for the selected scheduled scan.

3. Click **OK**.

5.6 Agent scheduled scans

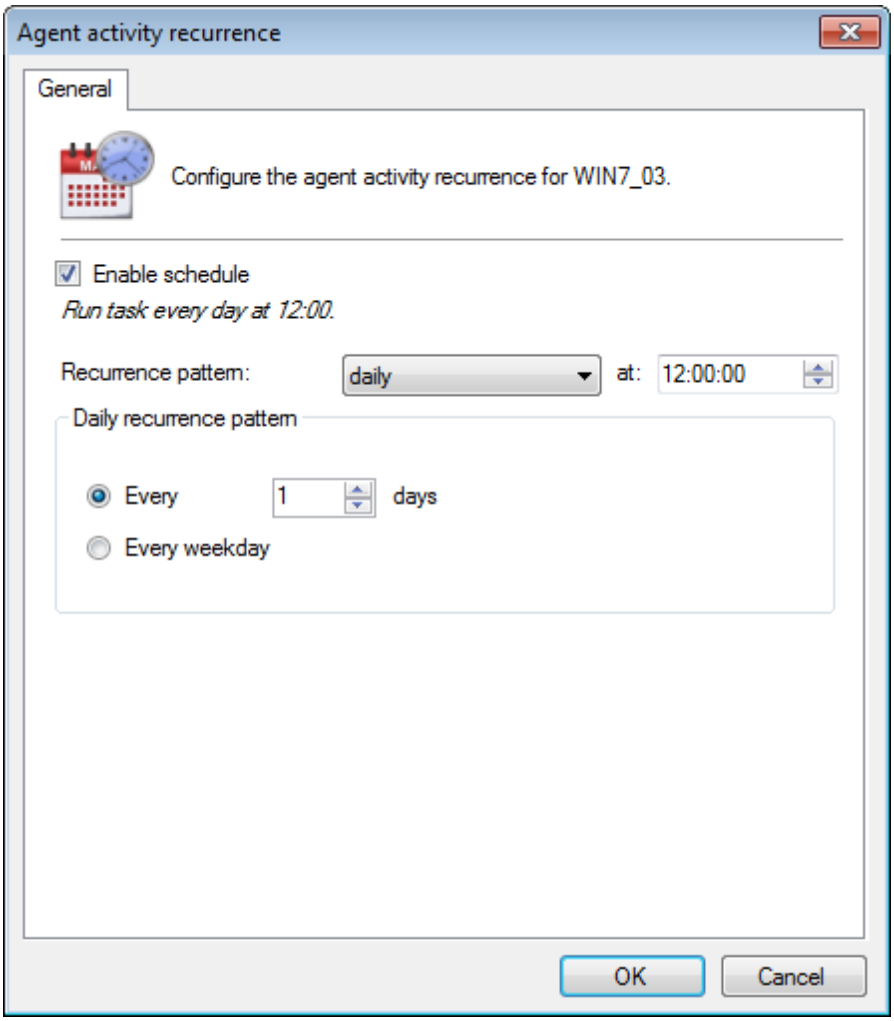
GFI LanGuard enables you to configure scheduled scans on computers running agents. Scheduling can be configured from the Agent properties dialog as follows:

1. Launch GFI LanGuard.

2. From the **Home** screen, select **View Dashboard**.

3. From the computer tree, right-click the computer/computer group you want to configure and select **Properties**.

4. Click **Agent Status tab > Change scan schedule....**



Screenshot 44: Agent Activity Recurrence

5. Select **Enable Schedule** and configure the recurrence pattern.

6. Click **OK**.

Note

Additional properties can be configured from the **Properties** dialog. For more information, refer to Agent properties (page 47).

5.6.1 Starting an Agent scan manually

To start an on demand scan on an agent computer:

1. Launch GFI LanGuard.
2. Click **View Dashboard** and select the computer(s) you want to start scanning.
3. From the **Agent Status** section, click **Scan Now**.

> **Note**
>
> **Scan Now** is only visible when the **Agent Status** is **Agent Installed**.

6 Dashboard

The **Dashboard** section provides you with extensive security information based on data acquired during audits. Amongst others, the Dashboard enables you to determine the current network vulnerability level, the top-most vulnerable computers, and the number of computers in the database.

Topics in this chapter:

6.1 Achieving results from the dashboard 83

6.2 Using the Dashboard 84

6.3 Using the Computer Tree 84

6.4 Using Attributes 88

6.5 Dashboard actions 90

6.6 Exporting issue list 91

6.7 Dashboard views 91

6.1 Achieving results from the dashboard

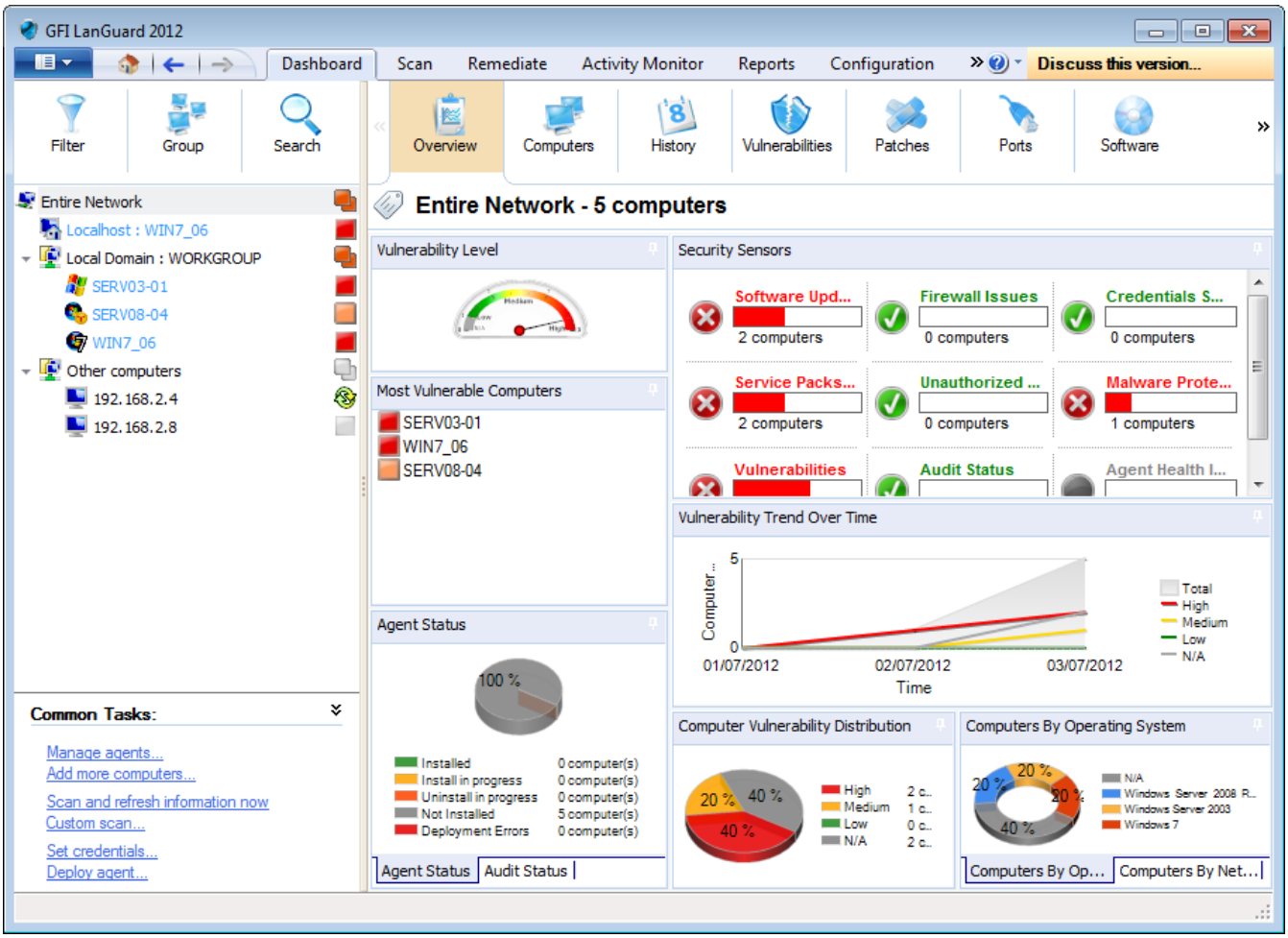
The dashboard is an important feature of GFI LanGuard. As the central point of the application, it enables you to perform all the common tasks supported by GFI LanGuard, including:

- Monitoring all computers managed by GFI LanGuard
- Managing scan targets. Add, edit or remove computers, domains and workgroups
- Deploying agents on scan targets and configure agent settings
- Configuring computer credentials
- Configuring auto-remediation options
- Configuring recurrent network discovery on the managed domains/workgroups/OUs
- Trigger security scans/refresh scan information
- Analyze computers security state and audit details
- Jump to relevant locations by clicking on security sensors and charts.

6.2 Using the Dashboard

This section provides the required information on how to use the GFI LanGuard Dashboard. To display the **Dashboard**:

1. Launch GFI LanGuard and click **Dashboard** tab.



Screenshot 45: View Dashboard

2. From the computers list, select a computer or computer group. The dashboard information updates according to your selection.

6.3 Using the Computer Tree

GFI LanGuard includes filtering and grouping options that enable you to quickly find a computer or domain and immediately display results.

When a computer or group is selected from the computer tree, results in the dashboard are automatically updated. Press **CRTL** and select multiple computers to display results for specific computers.

The following are functions supported by the computer tree:

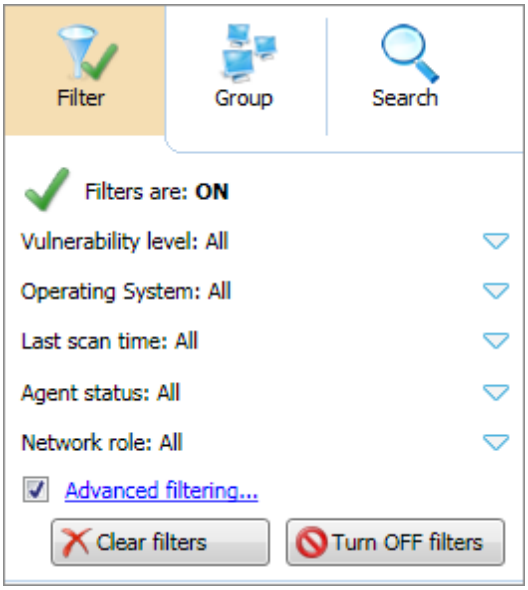
- Simple filtering
- Advanced filtering
- Grouping
- Searching

6.3.1 Simple filtering

To filter for a specific computer or group:

1. From the left pane, click **Filter**.

2. Configure the criteria and click **Turn ON filters**.



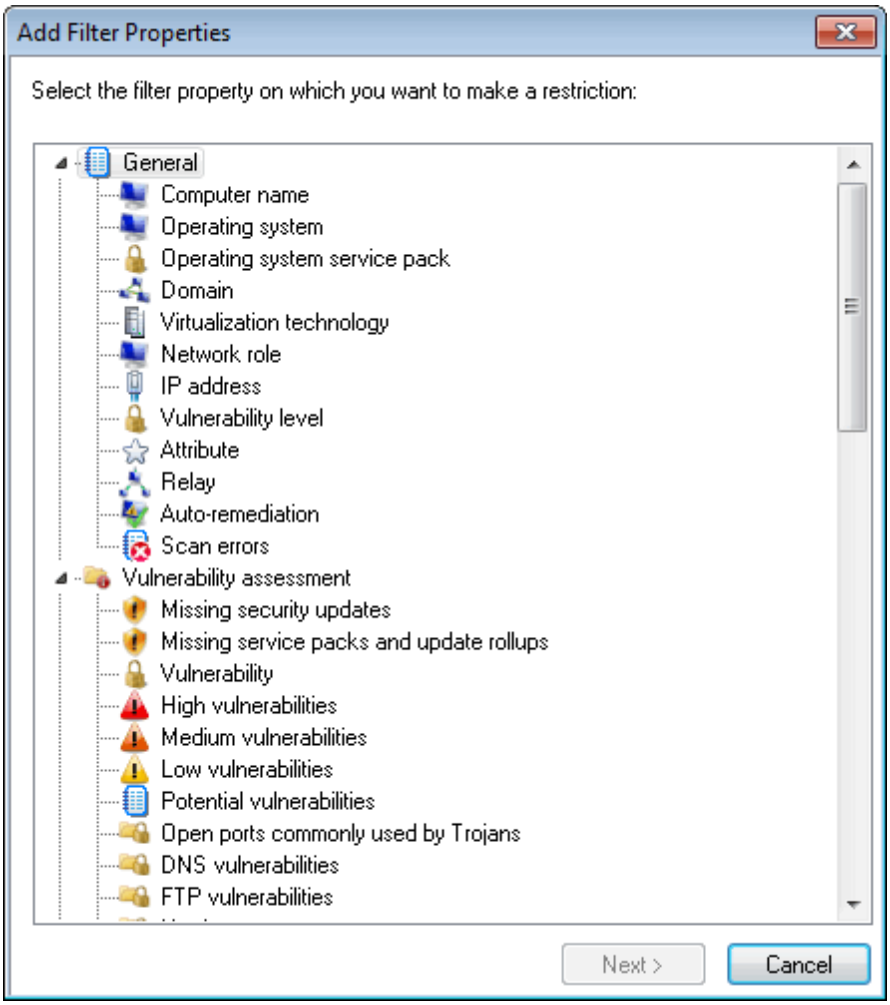
Screenshot 46: Simple filtering

6.3.2 Advanced filtering

To filter for a specific computer or group using advanced filtering:

1. From the left pane, click **Filter** and **Advanced filtering...**

2. From the **Advanced Filtering** dialog, click **Add**.



Screenshot 47: Add Filter Properties

3. Select the filter property to restrict and click **Next**.

4. Select the condition and key in the condition value. Click **Add**.

5. Repeat steps 2 to 4 for each condition. Click **OK**.

6.3.3 Grouping

To group machines by specific attributes:

1. From the left panel, click **Group**.

2. Select one of the following attributes:

- Domain and Organizational Unit
- Operating System
- Network Role
- Relays Distribution
- Attributes.

Note

If **Attributes** is selected, select the attribute from the drop down list. For more information, refer to Using Attributes (page 88).

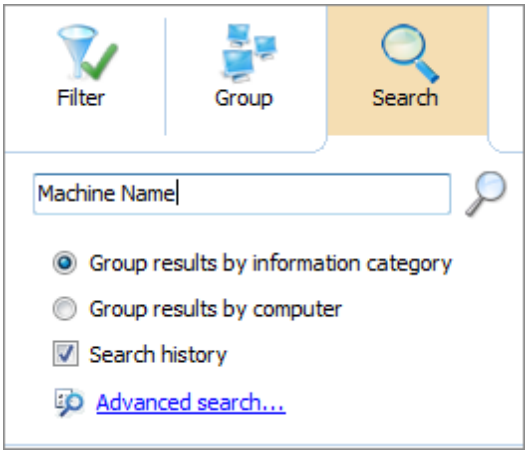
3. If Attributes is selected, select the attribute from the drop-down list.

4. Click **Apply grouping**.

6.3.4 Searching

The Search tab within the **Computers tree** enables you to search and display results for a specific computer or group. To display results for a specific computer:

1. From the **Computers tree**, select **Search**.



Screenshot 48: Search specific computers and groups

2. Key in the search criteria and use the following options:

Table 37: Search options

Option	Description
Group results by information category	Search results are grouped by category. The result contains the latest computer information. Amongst others results are grouped by: » Computer Information » Hardware devices » Logged on Users » Processes » Virtual technology
Group results by computer	Search results are grouped by computer name. The result contains the latest computer information.
Search History	Search results include the information from previous scans.
Advanced search	Configure advanced search options. **Note** For more information, refer to Full text searching (page 174).

6.4 Using Attributes

Attributes enable you to group and configure single or multiple computers at one go. Attributes also enable you to remediate vulnerabilities or deploy software on specific computers based on the assigned attribute. The following sections contain information about:

» Assigning attributes to a computer

» Assigning attributes to a group

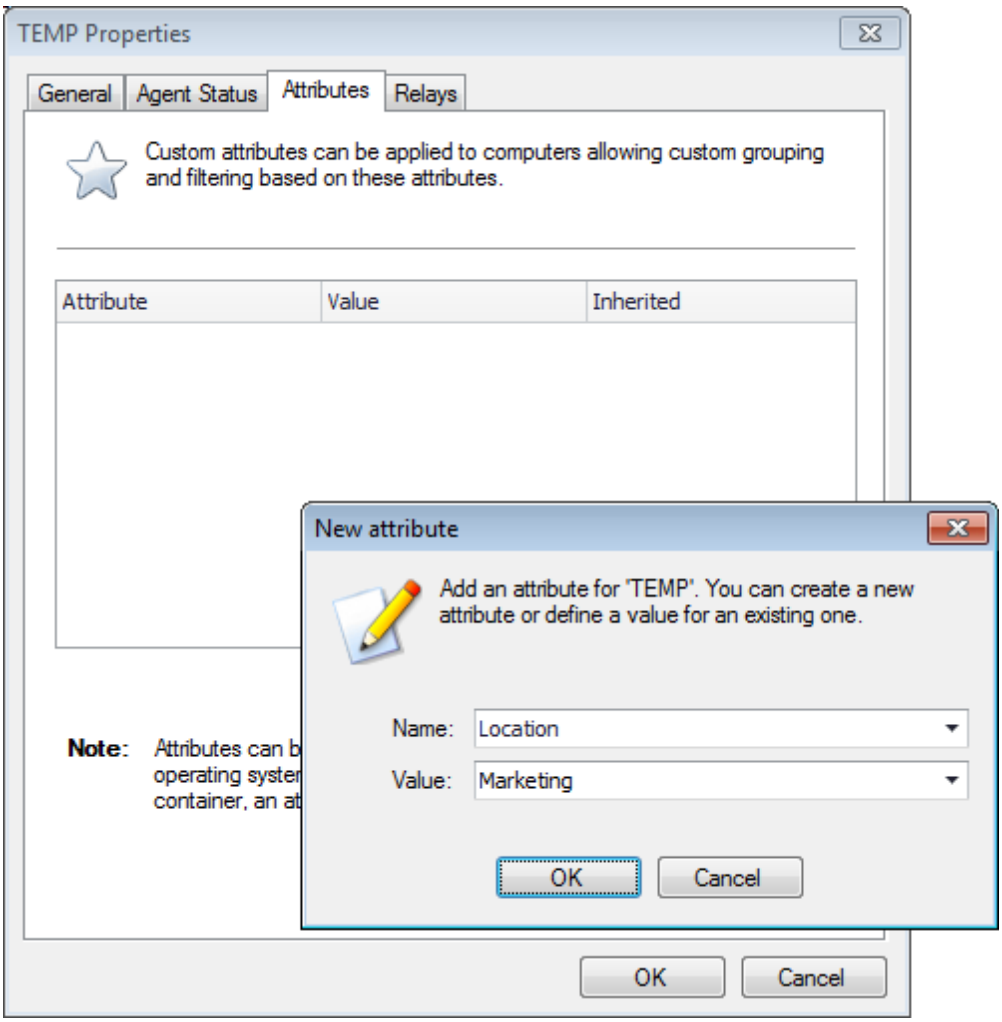
» Configuring attributes

6.4.1 Assigning attributes to a computer

To assign attributes to a single computer:

1. Click **Dashboard** tab.

2. From the computer tree, right-click a computer and select **Assign attributes**.



Screenshot 49: Assigning attributes: Single computer

3. From the **Properties** dialog > **Attributes** tab, click **Add**.

4. Configure new attributes settings and click **OK**.

5. Click **OK** to save your settings.

6.4.2 Assigning attributes to a group

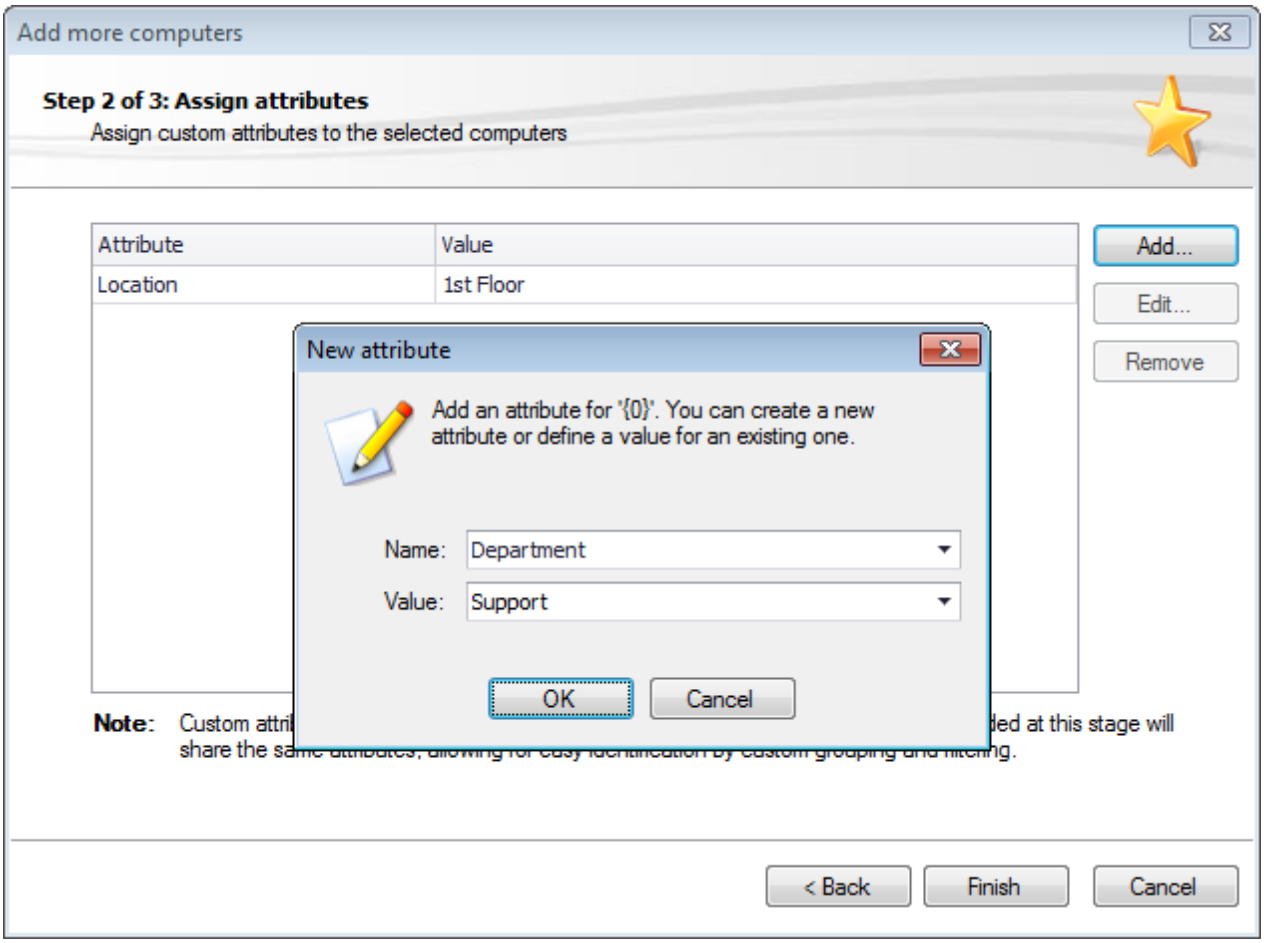
GFI LanGuard enables you to assign attributes to specific groups, domains, organizational units and networks. Once attributes are assigned, each member of the selected group inherits the attributes settings.

To assign attributes to a group:

1. Click **Dashboard** tab.

2. From the computers list, right-click network and select **Assign attributes**.

3. From the **Add more computers** wizard, select network and click **Next**.



Screenshot 50: Assigning attributes: Multiple computers

4. Click **Add** and configure the respective attributes. Use the **Edit** and **Remove** buttons to edit or remove the selected attributes.

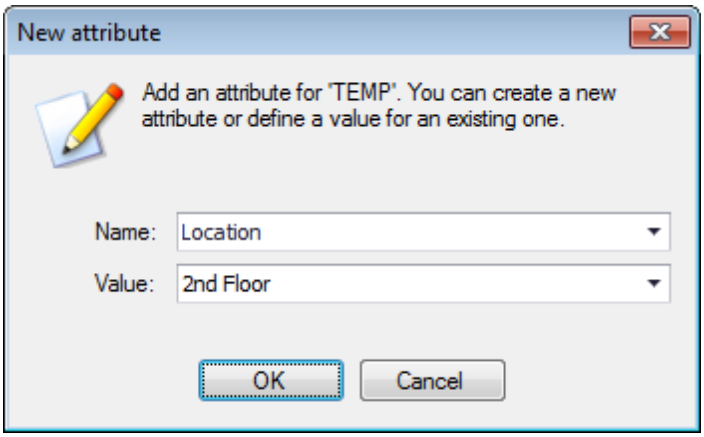
5. Click **Finish** to save your settings.

6.4.3 Configuring attributes

To configure attributes:

1. From the **Properties** dialog, click **Attributes** tab.

2. Click **Add** to launch the **New attribute** dialog.



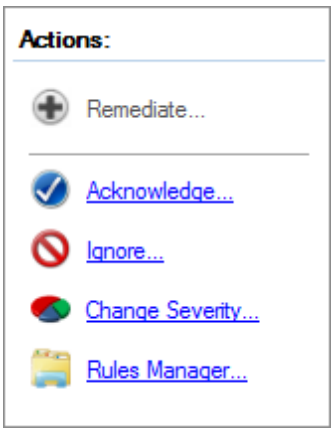
Screenshot 51: New attribute dialog

3. From the **Name** drop-down menu, select an attribute or key-in a name to create a new one.
4. Specify a value for the attribute in the **Value** field. Click **OK**.
5. Repeat steps 2 to 4 until you add all the required attributes.
6. Click **OK** to save your settings.

6.5 Dashboard actions

The **Actions** section enables you to manage and remediate vulnerabilities and missing patches found in your network. To access the **Actions** section:

1. Select **Dashboard** tab.
2. Click **Vulnerabilities** or **Patches** tab.



Screenshot 52: Actions section in the Dashboard

3. Select one of the following actions:

Table 38: Dashboard actions

Action	Description
Remediate	Launch the Remediation Center to deploy and manage missing patches. **Note** For more information, refer to Manual Remediation (page 138).
Acknowledge	Launch the Rule-Acknowledge Patch dialog. This enables you to acknowledge issues so that they will not affect the Vulnerability level of your network. Configure for which machine this rule applies

Action	Description
Ignore	Launch the Rule-Ignore Patch dialog. This enables you to ignore missing patches or vulnerabilities so that they will not be reported as issues in the future. Configure for which machine this rule applies and the time span that the issue is ignored.
Change Severity	Launch the Rule-Change Severity dialog. This enables you to change the severity level of vulnerability. Configure for which machines this rule applies and the severity level.
Rules Manager	Launch the Rules Manager dialog. This enables you to search and remove configured rules.

6.6 Exporting issue list

GFI LanGuard enables you to export issue lists to Portable Document Format (PDF), Microsoft Office Excel (XLS) or Hyper Text Markup Language (HTML). When a list supports exporting, these icons

are displayed in the top-right corner of the list. Select the respective icon and configure the export settings.

6.7 Dashboard views

The GFI LanGuard dashboard is made up of multiple views. These different views enable real-time monitoring of your scan targets and allow you to perform instant remedial and reporting operations. The following sections contain information about:

- Dashboard overview
- Computers view
- History view
- Vulnerabilities view
- Patches view
- Ports view
- Software view
- Hardware view
- System Information view

6.7.1 Overview

Screenshot 53: Dashboard Overview

The **Dashboard Overview** is a graphical representation of the security level/vulnerability level of a single computer, domain or entire network.

When a computer or domain is selected, the results related to the selected computer/domain are automatically updated in the dashboard. Below is a description of each section found in the dashboard:

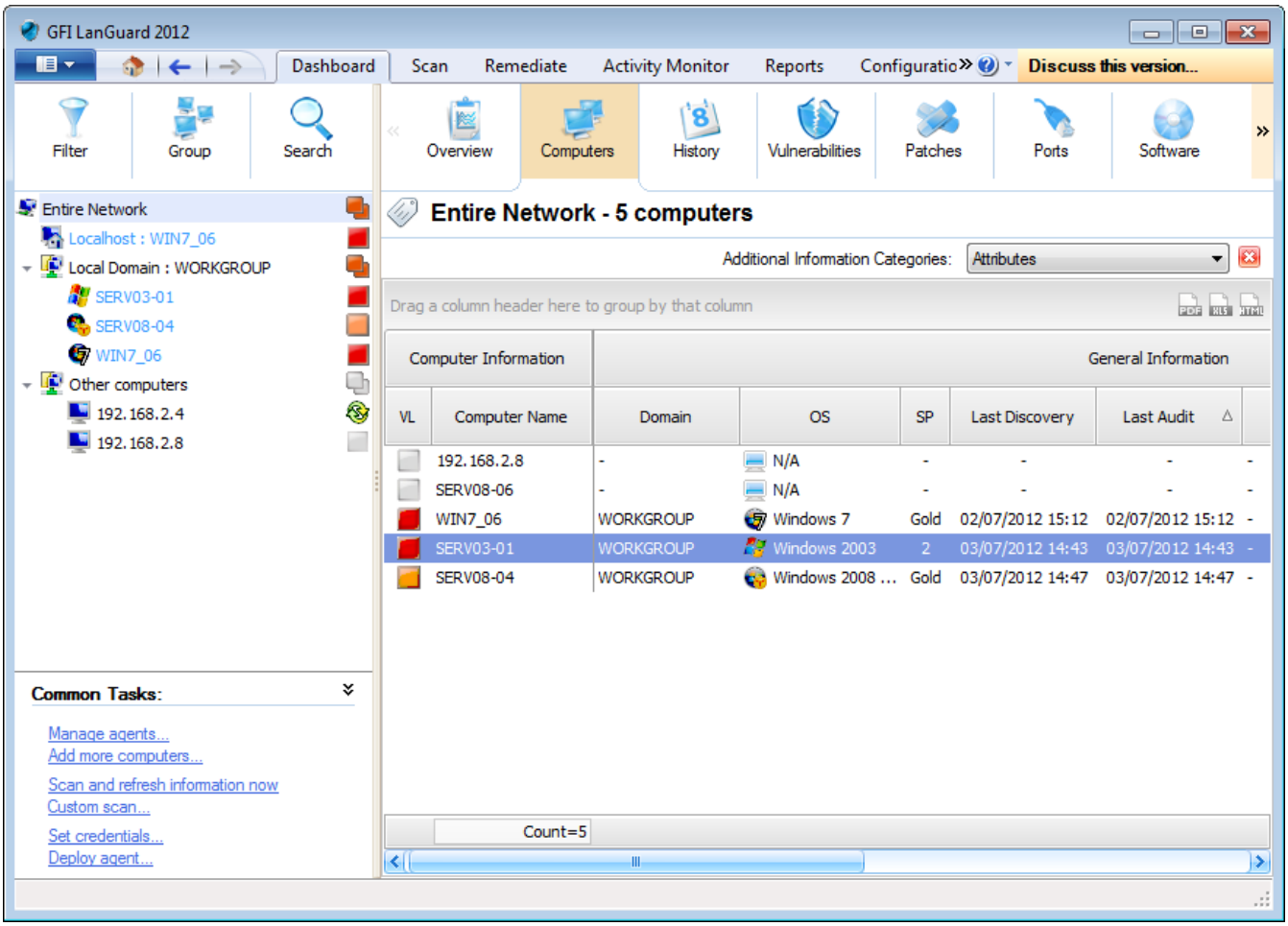
Table 39: Software information from an audit

Section	Description
Network security level	This rating indicates the vulnerability level of a computer/network, depending on the number and type of vulnerabilities and/or missing patches found. A high vulnerability level is a result of vulnerabilities and/or missing patches which average severity is categorized as high.
Computer vulnerability distribution	This chart is available only when selecting a domain or a workgroup, and displays the distribution of vulnerabilities on your network. This chart enables you to determine how many computers have high, medium and low vulnerability rating.
Most vulnerable computers	This list is available only when selecting a domain or a workgroup, and shows the most vulnerable computers discovered during the scan. The icon color on the left indicates the vulnerability level.

Section	Description
Agent Status	When selecting a domain or workgroup, a chart showing the overall agent status of all computers within the domain/workgroup is displayed. This enables you to determine the number of agents installed or pending installation on the selected domain/workgroup. When selecting a single computer, this section displays an icon representing the agent status. The icons are described below: » **Not installed** - Agent is not installed on the target machine. » **Pending installation** - Installation is pending. A status can be pending when the machine is offline or the agent is being installed. » **Pending uninstall** - Uninstallation is pending. A status can be pending when the machine is offline or the agent is being uninstalled. » **Installed** - Agent is installed on the target machine. » **Relay Agent Installed** - The selected computers are relay agents.
Audit status	This chart is available only when selecting a domain or workgroup and enables you to identify how many audits have been performed on your network grouped by time.
Vulnerability trends over time	When a domain or workgroup is selected, this section displays a line graph showing the change of vulnerability level over time grouped by computer count. When a single computer is selected, this section displays a graph showing the change of vulnerability level over time for the selected computer.
Computers by network role	This chart is available only when selecting a domain or a workgroup and displays the number of audited computers, grouped by network role. Amongst other roles, this graph identifies the number of servers and workstations per selected domain.
Computers by operating system	This chart is available only when selecting a domain or a workgroup and displays the number of audited computers, grouped by the installed operating system.
Computer details	This section is available when selecting a single computer and enables you to view the selected computer details.
Scan activity	This line graph is available only when selecting a single computer and enables you to view the number of scans/audits performed on the selected computer. In addition enables you to verify if scheduled scans are being performed.
Remediation Activity	This line graph is available only when selecting a single computer and enables you to view the number of remediation activities performed on the selected computer. In addition, this graph enables you to verify that auto-remediation is performed.
Top 5 Issues to Address	This section is available only when selecting a single computer, and displays the top five issues to address for the selected computer.
Results statistics	This section is available only when selecting a single computer and displays an overview of the audit result. Amongst others, the result enables you to identify the number of missing patches, number of installed applications, open ports and running services.

Section	Description
Security Sensors	This section enables you to identify issues at a glance. Click a sensor to navigate and display issues and vulnerabilities for a specific computer or group. Sensors enable you to identify: » Missing Software Updates » Missing service packs » Vulnerabilities » Firewall Issues » Unauthorized Applications » Audit Status » Credentials setup » Malware Protection Issues » Agent Health Issues.

6.7.2 Computers view



Screenshot 54: Analyze results by computer

Select this view to group audit results by computer. From the drop-down list, select one of the options described below:

Table 40: View by computers information

Option	Description
Agent Details	Select this option to view the agent status. This option enables you to identify if an agent is installed on a computer and if yes, displays the type of credentials being used by the agent.
Vulnerabilities	View the number of vulnerabilities found on a computer grouped by severity. Severity of a vulnerability can be: » High » Medium » Low » Potential.
Patching status	View the number of: » Missing Security/non-Security Updates » Missing Service Packs and Update Rollups » Installed Security/non-Security Updates » Installed Service Packs and Updates Rollups.

Option	Description
Open ports	View the number of: » Open TCP ports » Open UDP ports » Backdoors.
Software	View the number of: » Antiphishing engines » Antispyware engines » Antivirus engines » Backup applications » Data loss prevention applications » Device access and desk encryption applications » Firewalls » Installed applications » Instant messengers » Peer to peer applications » Unauthorized applications » Virtual machines » VPN clients » Web browsers.
Hardware	View information on: » Number of disk drives » Free disk space » Memory size » Number of processors » Other hardware.
System information	View information on: » The number of shared folders » Number of groups » Number of users » Logged users » Audit policy status.
Attributes	Adds an **Attributes** column and groups your scan targets by the assigned attribute.

Note

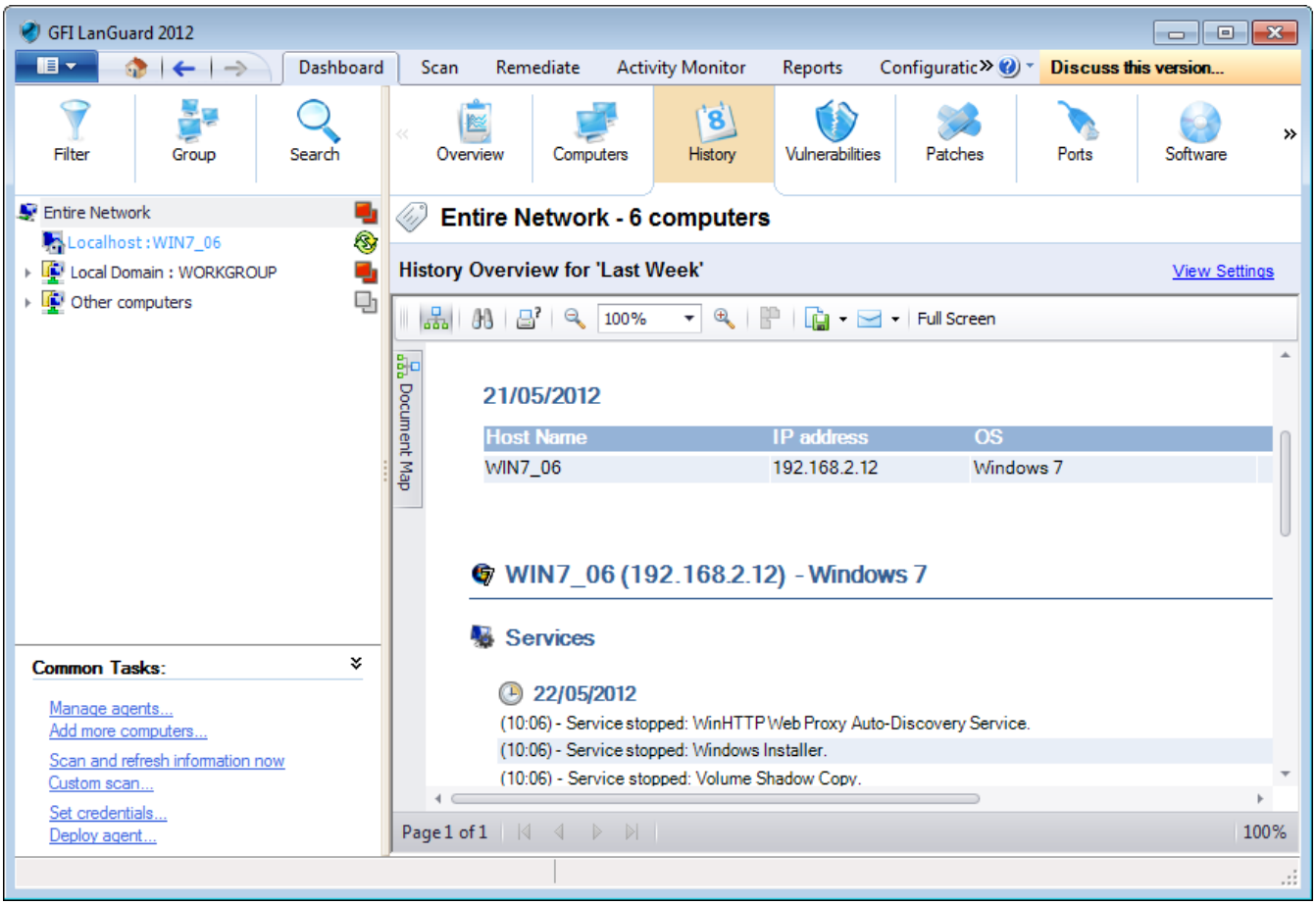
To launch the **Overview** tab and display more details on a specific computer, double click a computer from the list.

Note

Drag and drop a column header in the designated area to group data by criteria.

6.7.3 History view

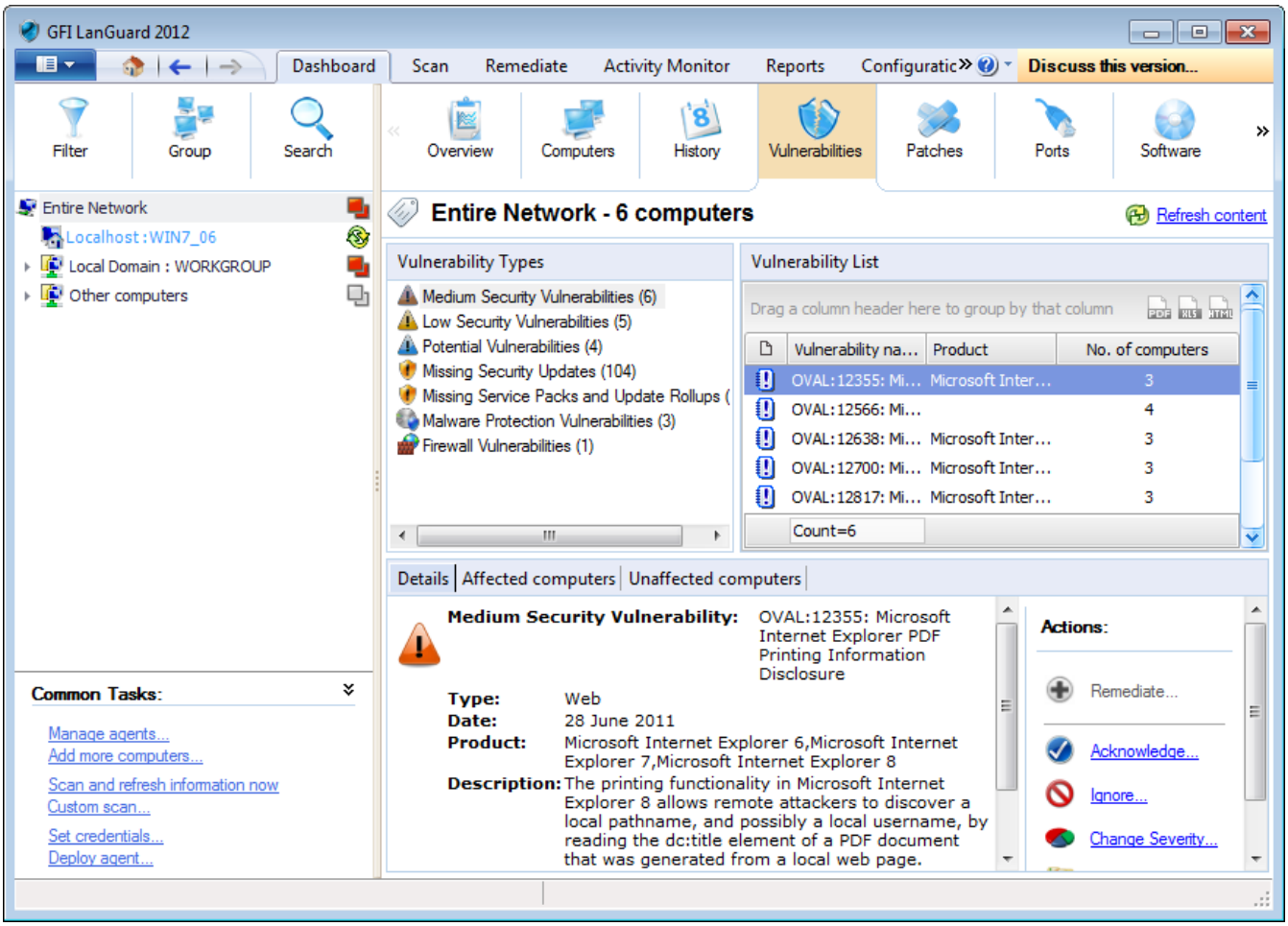
Select this view to group audit results by date for a specific computer. To configure the history starting date or history period click the link provided.



Screenshot 55: History view in the Dashboard

6.7.4 Vulnerabilities View

Display more details on the vulnerabilities found on a network and the number of affected computers. When a vulnerability is selected from the **Vulnerability** List, the **Details** section provides more information on the selected vulnerability. From the **Details**, section click **Affected computers** or **Unaffected computers** to display a list of affected and unaffected computers.



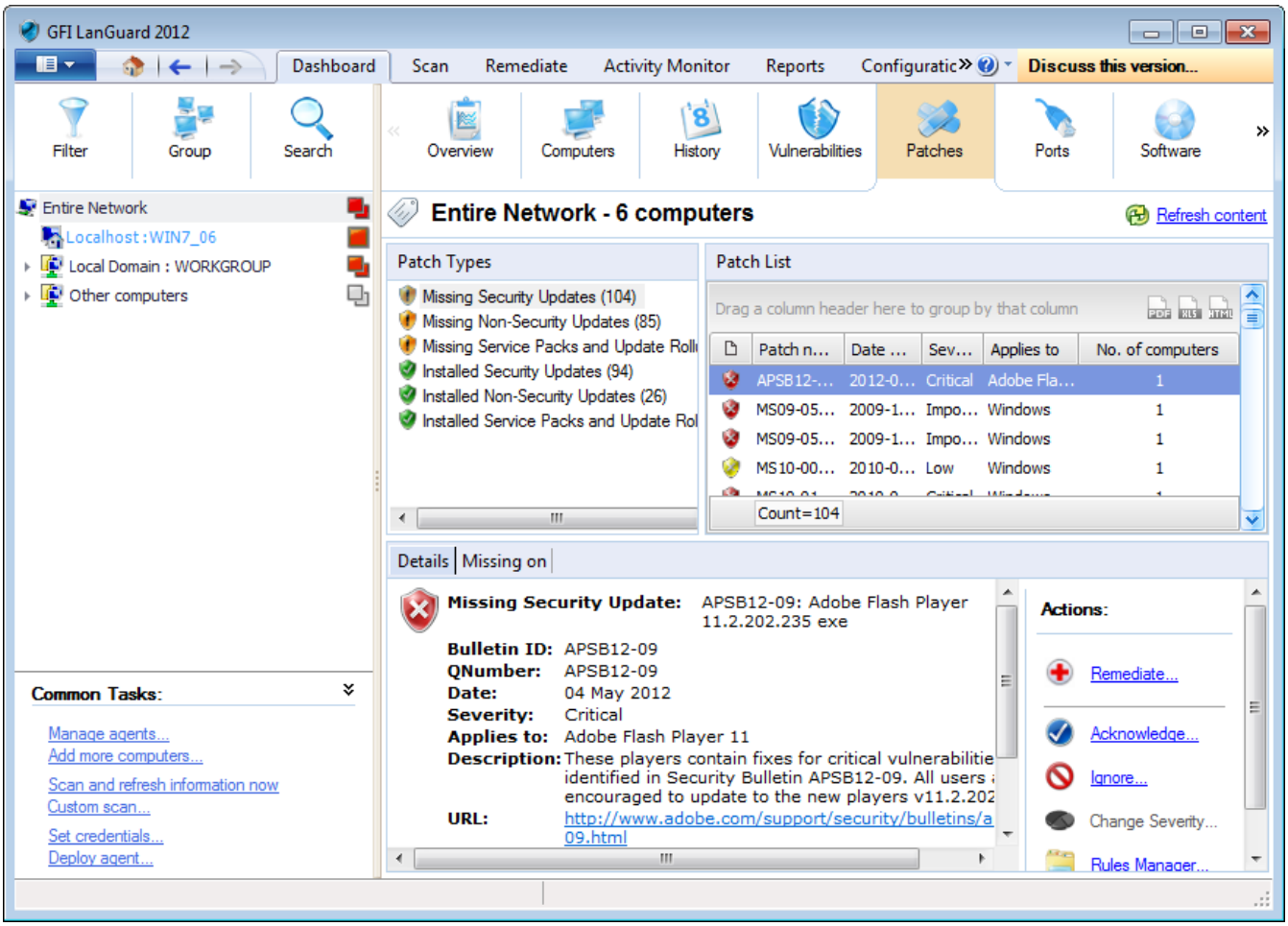
Screenshot 56: Vulnerabilities view in the Dashboard

Note

Drag and drop a column header in the designated area to group data by criteria.

6.7.5 Patches View

Display more details on the missing/installed patches and service packs found during a network audit. When a patch/service pack is selected from the list, the **Details** section provides more information on the selected patch/service pack. From the **Details** section, click **Missing on** to display a list of computers having the selected patch missing.



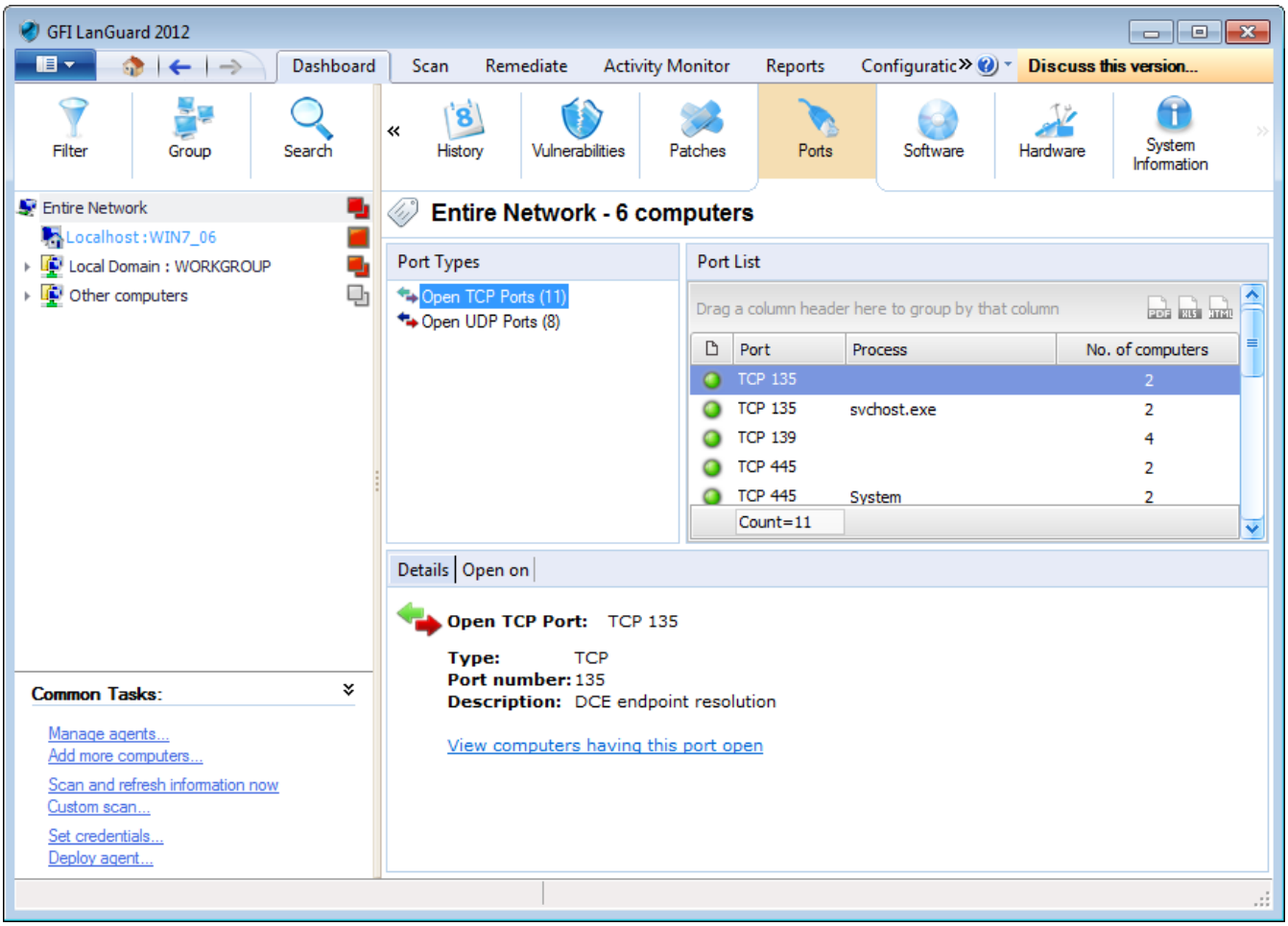
Screenshot 57: Patches view in Dashboard

Note

Drag and drop a column header in the designated area to group data by criteria.

6.7.6 Ports View

Display more details on the open ports found during a network audit. When a port is selected from the **Port** List, the **Details** section provides more information on the selected port. From the **Details** section, click **View computers having this port open** to display a list of computers having the selected port open.



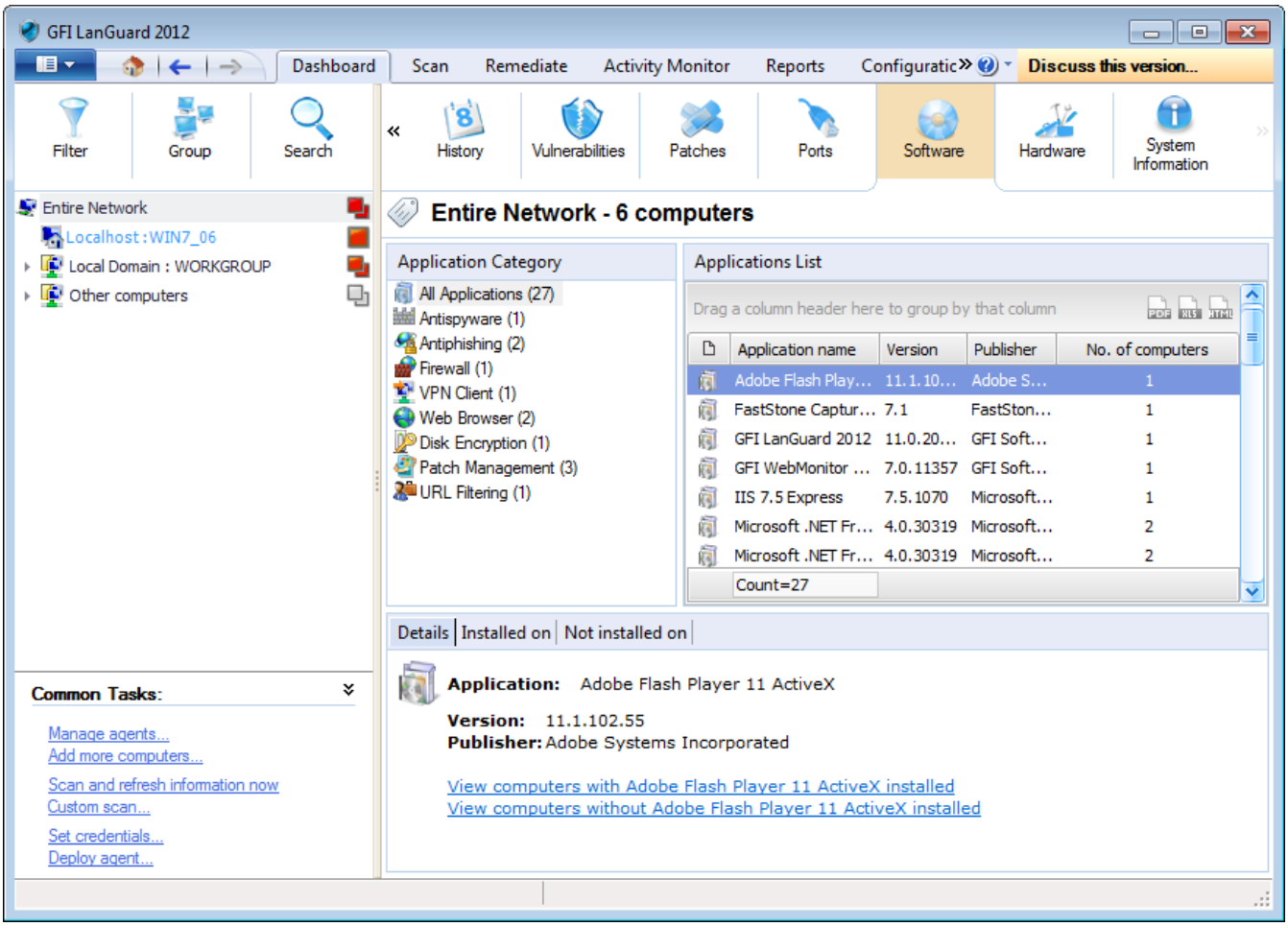
Screenshot 58: Ports view in Dashboard

Note

Drag and drop a column header in the designated area to group data by criteria.

6.7.7 Software View

Display more details on the installed applications found during a network audit. When an application is selected from the **Application** List, the **Details** section provides more information on the selected application.



Screenshot 59: Software view in Dashboard

Note

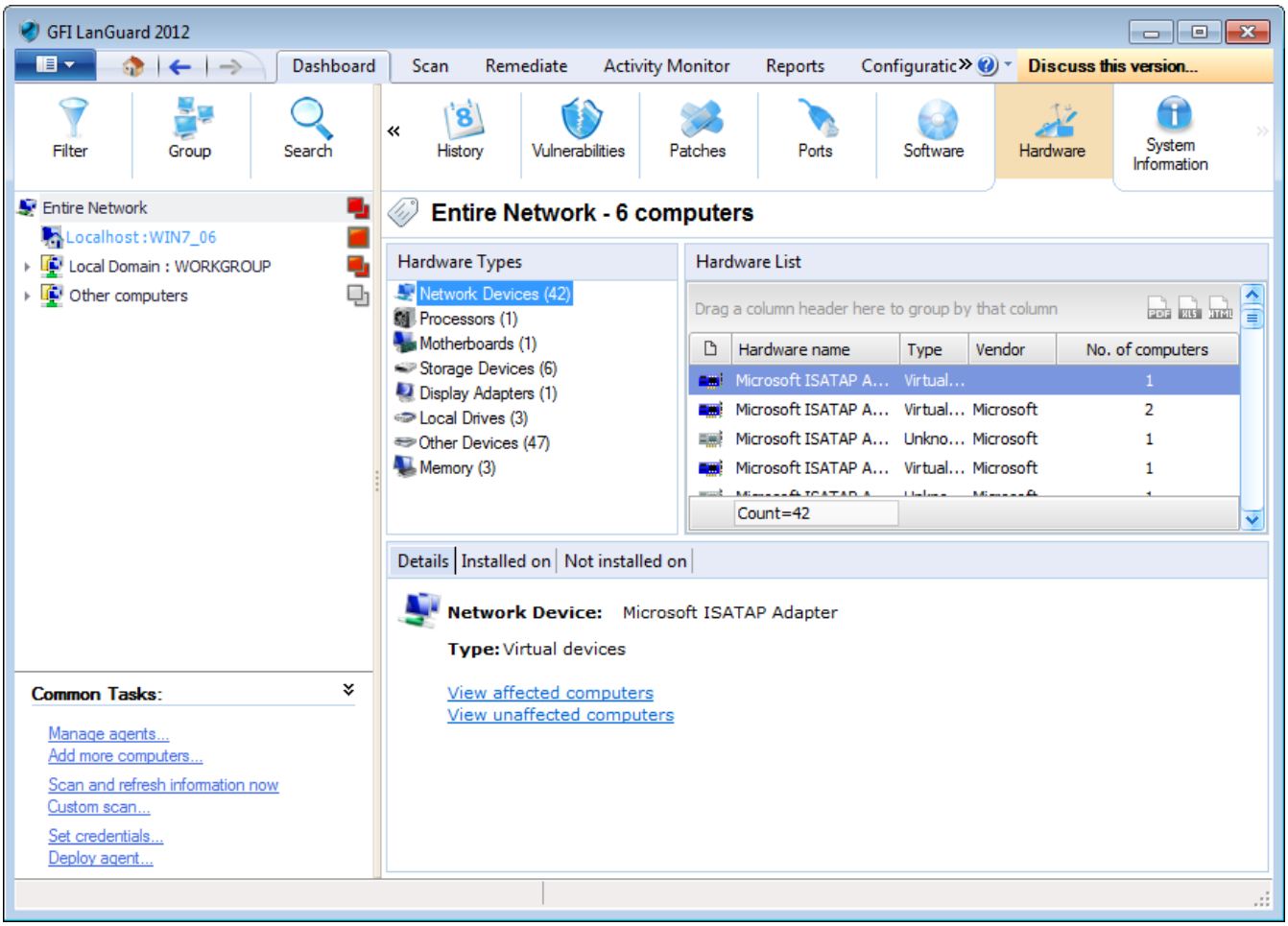
Drag and drop a column header in the designated area to group data by criteria.

Note

Agent-less scans require to temporarily run a service on the remote machine. **Select Enable full security applications audit...** to enable this service on all agent-less scanning profiles.

6.7.8 Hardware View

Display more information on the hardware found during a network audit. Select hardware from the list to display more details.



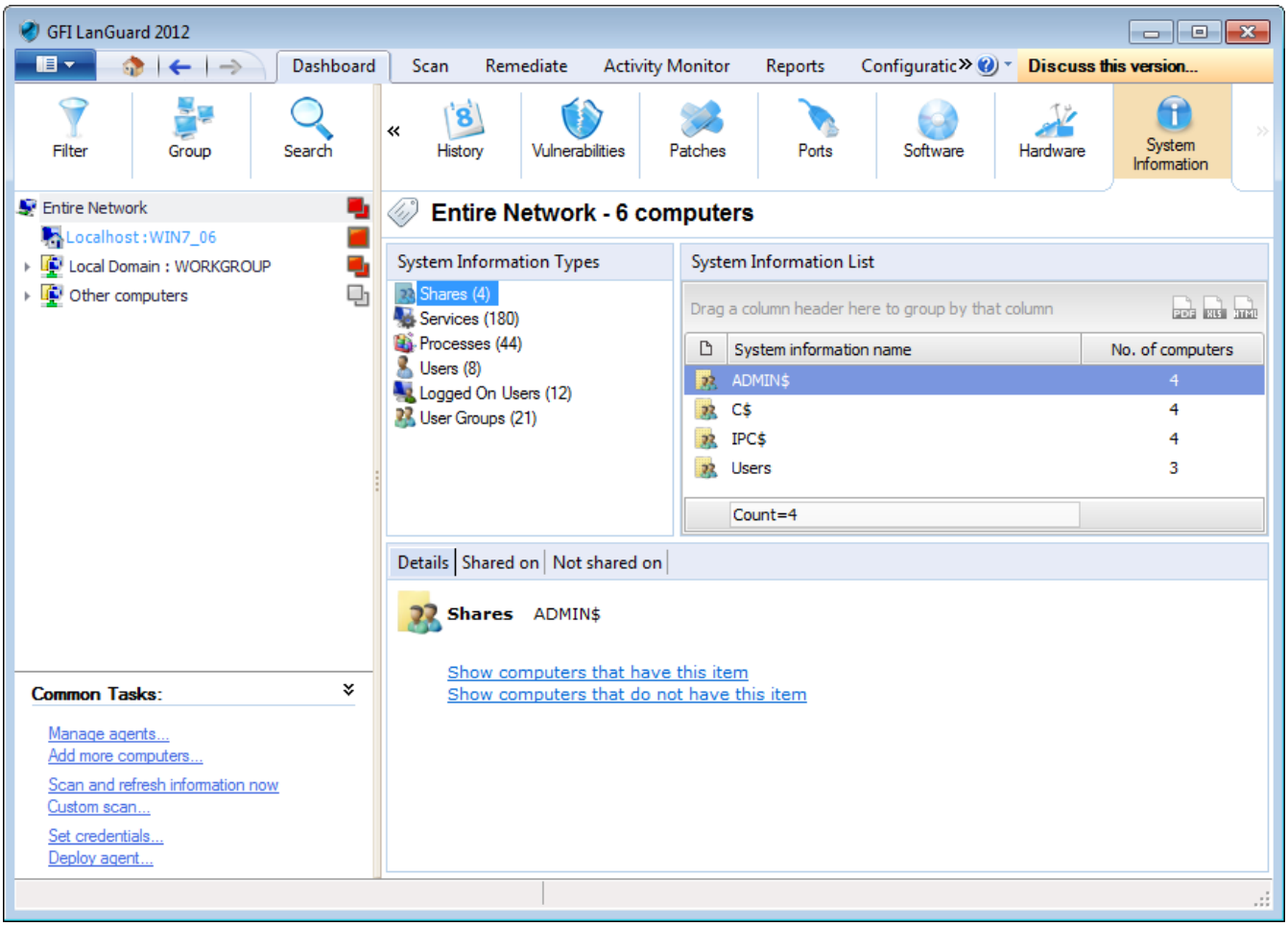
Screenshot 60: Hardware view in Dashboard

Note

Drag and drop a column header in the designated area to group data by criteria.

6.7.9 System Information View

The **System Information** tab, displays information associated with the operating system of a scan target(s).



Screenshot 61: System Information view in Dashboard

Note

Drag and drop a column header in the designated area to group data by criteria.

7 Interpreting Results

On completion of a network security scan, it is important to identify the areas that require immediate attention. Use the information provided in this chapter to determine the correct analysis and interpretation approach to get the most out of your scan results and apply the appropriate fixes.

Topics in this chapter:

7.1 Interpreting manual scan results 104

7.2 Loading results from the database 113

7.3 Saving and loading XML results 114

7.1 Interpreting manual scan results

The **Scan Results Overview** and **Scan Results Details** sections in the **Scan** tab, are designed to facilitate the result analysis process as much as possible. Use the information in the following sections to learn how scan results are interpreted and know which areas require your immediate attention:

- Viewing scan results
- Vulnerability level rating
- Vulnerability Assessment
- Network & Software Audit

7.1.1 Viewing scan results

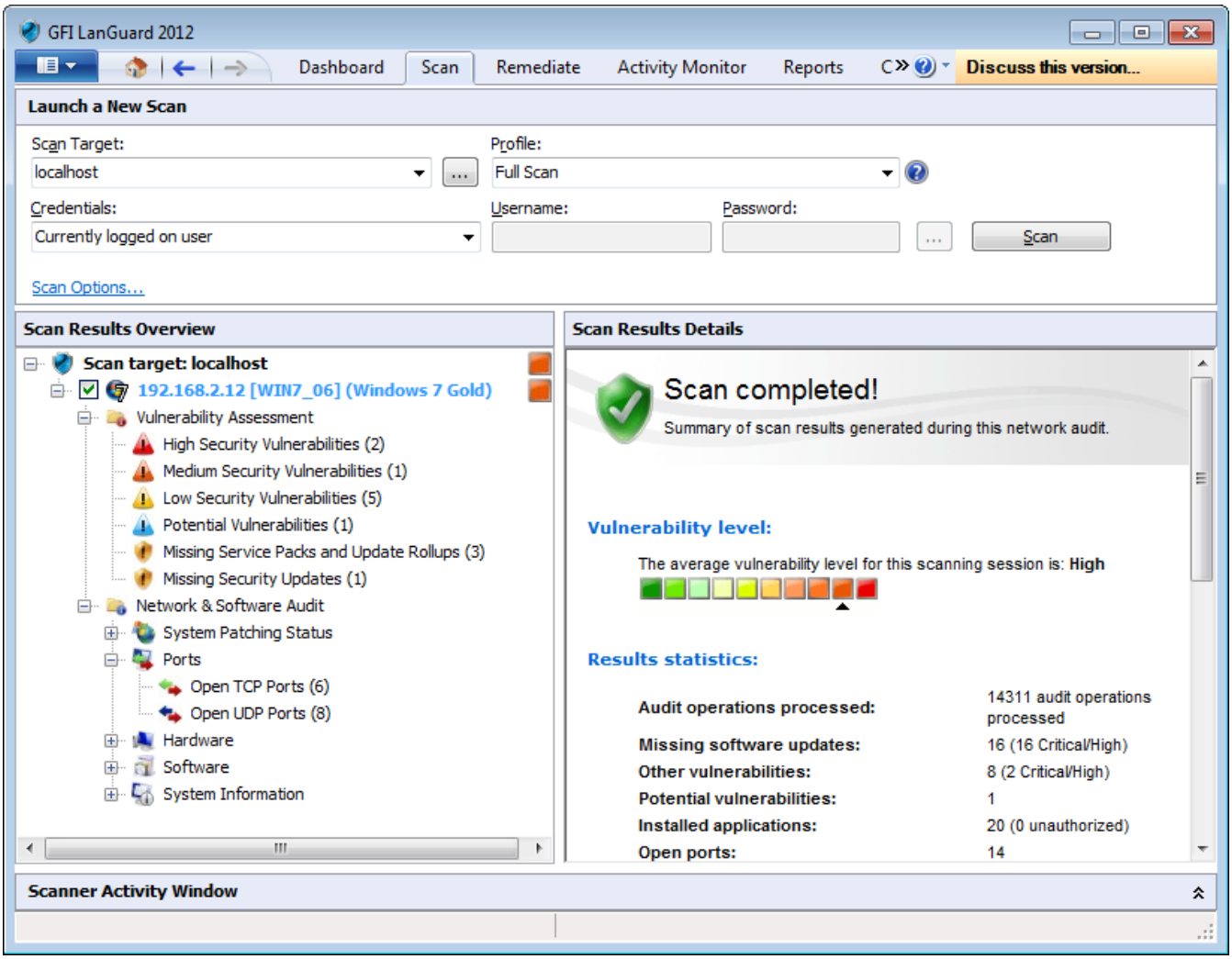
Use this section to interpret results generated by manual scans and results stored in the database backend. For more information, refer to Manual scans (page 66).

To view manual scan results:

1. Launch GFI LanGuard and click the **Scan** tab.

2, Launch a new scan or load the result from the database/file. For more information, refer to Loading results from the database (page 113).

3. Once completed, the results are displayed in the **Scan Result Overview** and the **Scan Results Details** sections.



Screenshot 62: Results overview

From **Scan Results Overview**, expand a computer node to access results retrieved during the scan. Security scan results are organized in two sub-nodes tagged as:

- Vulnerability Assessment
- Network & Software Audit

While a scan is in progress, each computer node has an icon that categorizes the response time. The table below describes the different icons used by GFI LanGuard to categorize the response time. The first icon indicates that the scan is queued, while the second icon indicates that the scan is in progress.

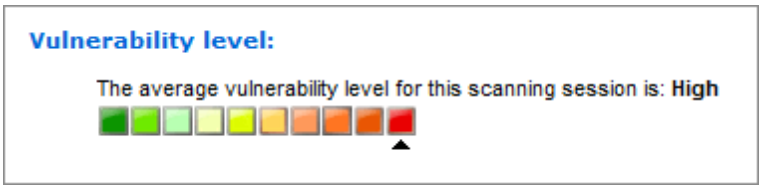
Table 41: Response time icons

Category	Information	Description
	Fast response	Less than 25ms
	Medium response	Between 25ms and 100ms
	Slow response	More than 100ms

7.1.2 Vulnerability Level Rating

The GFI LanGuard vulnerability level is a rating assigned to each scanned computer. The rating can be viewed from:

- **Scan Results Details** – This section in the Scan tab provides you with a vulnerability level meter assigned the computers/groups that have been scanned
- **Dashboard** – The Dashboard section provides you with information for specific computers or selected groups of computers, from the computer tree. Select the computer/group and view the vulnerability meter from the right pane. Select Entire Network to view the vulnerability level for all your scan targets.



Screenshot 63: Vulnerability level meter

How is the vulnerability level calculated?

The vulnerability level is calculated using a weighting system. After a scan, GFI LanGuard groups the discovered vulnerabilities in categories sorted by severity rating:

- High
- Medium
- Low

For each rating, a weighted score is given. This is based on the total number of vulnerabilities per category.

> **Note**
>
> When the vulnerability level cannot be assessed and/or vulnerability scanning was not performed, GFI LanGuard gives a rating of **N/A**.

Weight scores

Table 42: Vulnerability level weight scores

Category	Number of Detected Vulnerabilities	Scores
High Vulnerabilities	1-2	8
	3-5	9
	> 5	10
Medium Vulnerabilities	1-2	5
	3-5	6
	> 5	7
Low Vulnerabilities	1-2	2
	3-5	3
	> 5	4

Score classification

After categorizing detected vulnerabilities and generating a score for each category, the overall vulnerability level is generated. The vulnerability level is the severity rating with the highest score.

Vulnerability level scores:

- A score of >= **8**, results in **High** vulnerability rating
- A score of <= **7** and >= **5**, results in **Medium** vulnerability rating
- A score of <= **4** and >=**1**, results in a **Low** vulnerability rating.

Example

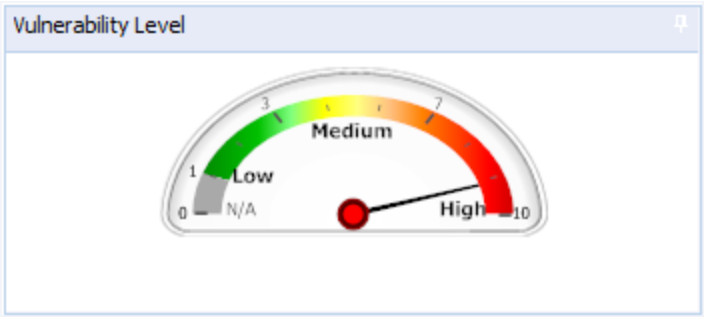
During a scan of Computer A, the following vulnerabilities were discovered:

- 3 high vulnerabilities
- 8 medium vulnerabilities
- 5 low vulnerabilities.

The score for each category was calculated by GFI LanGuard and returned the following results:

- 3 high vulnerabilities = 9
- 8 medium vulnerabilities = 7
- 5 low vulnerabilities = 3.

The vulnerability level for Computer A is therefore **HIGH**.

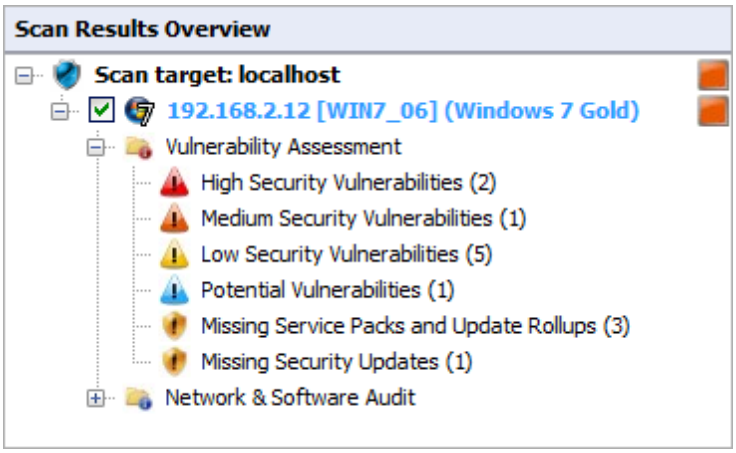


Screenshot 64: Dashboard Vulnerability Meter

The vulnerability level is indicated using color-coded graphical bar:

- Red bar = high vulnerability level
- Green bar = low vulnerability level.

7.1.3 Vulnerability Assessment



Screenshot 65: The Vulnerability Assessment node

Click on any **Vulnerability Assessment** node to view the security vulnerabilities identified on the target computer grouped by type and severity.

High Security Vulnerabilities

Click on the **High Security Vulnerabilities** or **Low Security Vulnerabilities** sub-nodes for a list of weaknesses discovered while auditing a target device. Groups are described in the following table:

Table 43: Vulnerability groups

Group	Description
Mail, FTP, RPC, DNS and Miscellaneous	Shows vulnerabilities discovered on FTP servers, DNS servers, and SMTP/POP3/IMAP mail servers. Links to Microsoft® Knowledge Base articles or other support documentation are provided.
Web	Lists discovered vulnerabilities on web servers (such as wrong configuration issues). Supported web servers include Apache, Internet Information Services (IIS®) and Netscape.
Services	Lists vulnerabilities discovered in active services as well as the list of unused accounts that are still active and accessible on scanned targets.
Registry	Registry settings of a scanned network device are listed. Links to support documentation and short vulnerability descriptions are provided.
Software	Enumerates software installed on the scanned network device(s). Links to supporting documentation and short vulnerability descriptions are provided.
Rootkit	Enumerates discovered vulnerabilities because of having a rootkit installed on the scanned network device(s). Links to supporting documentation and short vulnerability descriptions are provided.

Potential vulnerabilities

Select **Potential vulnerabilities** sub-node to view scan result items classified as possible network weaknesses. Although not classified as vulnerabilities, these scan result entries still require particular attention since malicious users can exploit them during malicious activity.

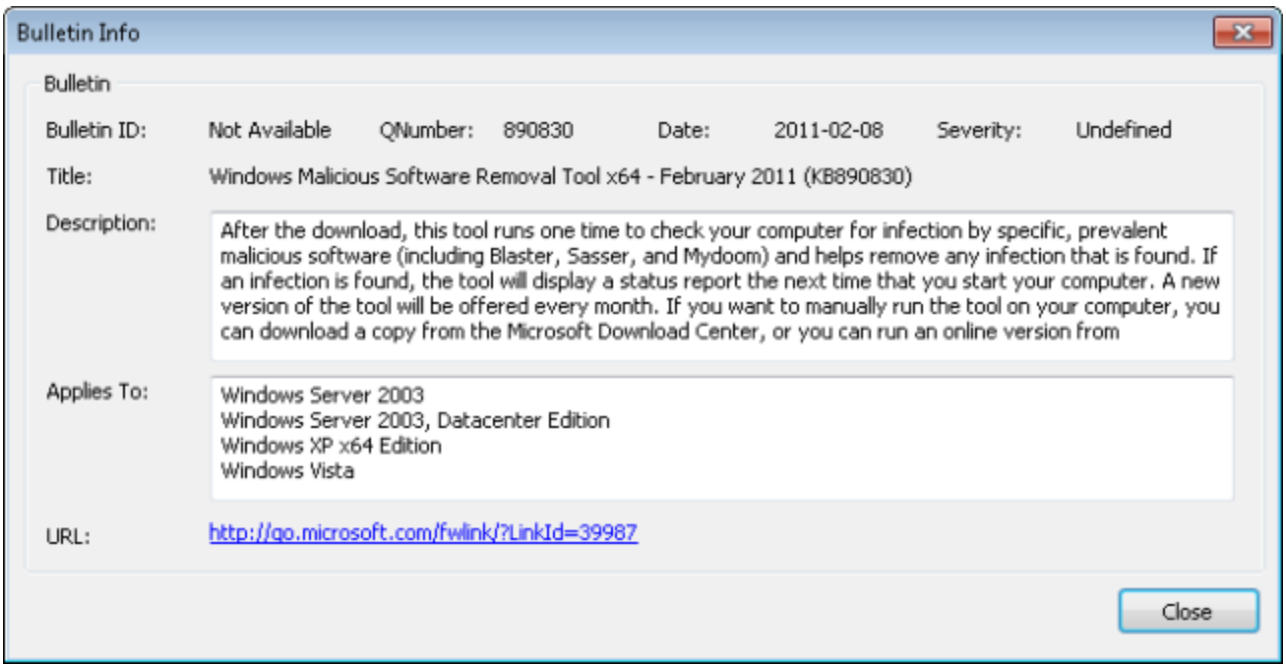
For example, during vulnerability scanning GFI LanGuard enumerates all modems installed and configured on target computers. If unused, modems are of no threat to your network. If connected to a telephone line these modems can however be used to gain unauthorized and unmonitored access to the Internet. Users can potentially bypass corporate perimeter security including firewalls, anti-virus, website rating and web content blocking. This exposes the corporate IT infrastructure to a wide range of threats including hacker attacks. GFI LanGuard considers installed modems as possible threats and enumerates them in the **Potential Vulnerabilities** sub-node.

Missing Service Packs

Click **Missing Service Packs and Update Rollups** or **Missing Security Updates** sub-nodes to check any missing software updates or patches. For a full list of missing service packs and missing patches that can be identified by GFI LanGuard, refer to http://go.gfi.com/?pageid=ms_app_fullreport

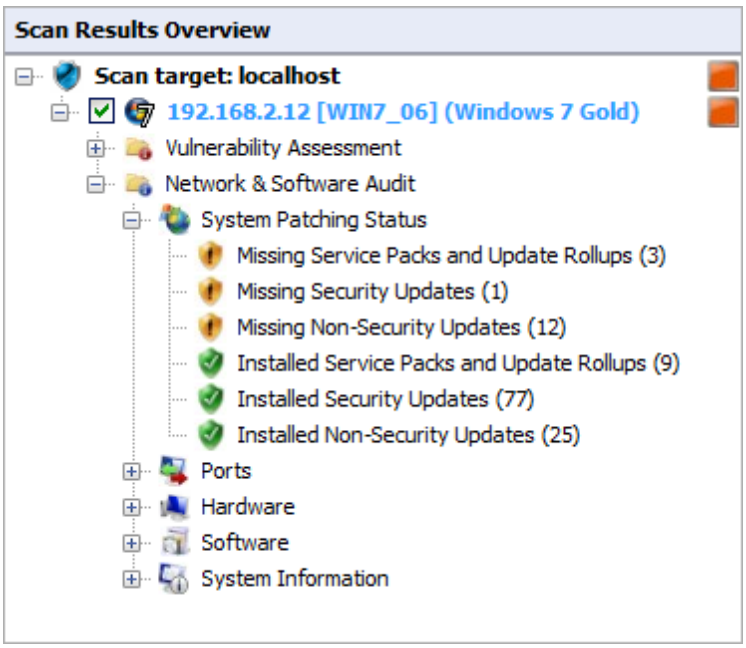
Bulletin information.

To access bulletin information, right-click on the respective service pack and select **More details > Bulletin Info**.


Bulletin Info
Bulletin
Bulletin ID: Not Available
QNumber: 890830
Date: 2011-02-08
Severity: Undefined
Title: Windows Malicious Software Removal Tool x64 - February 2011 (KB890830)
Description:
After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from
Applies To:
Windows Server 2003
Windows Server 2003, Datacenter Edition
Windows XP x64 Edition
Windows Vista
URL:
http://go.microsoft.com/fwlink/?LinkId=39987
Close

Screenshot 66: Bulletin info dialog

7.1.4 Network & Software Audit



Screenshot 67: The network and software audit node

Click **Network & Software Audit** to view security vulnerabilities identified on scanned targets. In this section, vulnerabilities are grouped by type and severity.

System Patching Status

Click **System Patching Status** to view all missing and installed patches on a target machine. Available links are:

- Missing Service Packs and Update Rollups
- Missing Security Updates
- Missing Non-Security Updates
- Installed Service Packs and Update Rollups
- Installed Security Updates
- Installed Non-Security Updates.

Scan Results Details
System Patching Status
Select one of the following system patching status categories bellow
Missing Service Packs and Update Rollups (3)
Allows you to analyze the missing service packs information
Missing Security Updates (1)
Allows you to analyze the missing security updates information
Missing Non-Security Updates (12)
Allows you to analyze the non-security updates information
Installed Service Packs and Update Rollups (9)
Allows you to analyze the installed service packs information
Installed Security Updates (77)
Allows you to analyze the installed security update information
Installed Non-Security Updates (25)
Allows you to analyze the installed non-security updateinformation

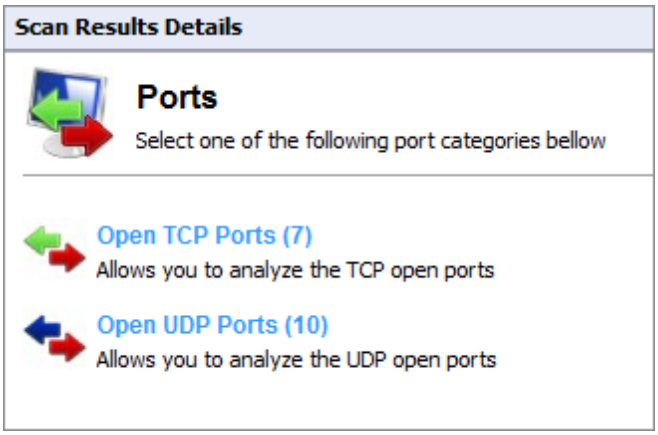
Screenshot 68: System patches status

Ports

Click **Ports** to view all open TCP and UDP ports detected during a scan. If a commonly exploited port is discovered to be open, GFI LanGuard marks it in red.

> **Note**
>
> Some software products may use the same ports as known Trojans. For additional security, GFI LanGuard identifies these ports as a threat.

Apart from detecting open ports, GFI LanGuard uses service fingerprint technology to analyze the service(s) that are running behind the detected open port(s). With service fingerprint, GFI LanGuard can detect if malicious software is using the detected open port.


Scan Results Details
Ports
Select one of the following port categories bellow
Open TCP Ports (7)
Allows you to analyze the TCP open ports
Open UDP Ports (10)
Allows you to analyze the UDP open ports

Screenshot 69: All UDP and TCP ports, found during a scan

Hardware

Click **Hardware** to view all details discovered by the hardware audit. The hardware audit, amongst others, displays information such as MAC addresses, IP addresses, device type; device vendor etc. The table below describes the hardware information groups:

Table 44: Hardware information from an audit

Information	Description
Network Devices	Includes information of all physical, virtual and software-enumerated devices.
Local Drives	Includes information on local drives such as available disk space and file system type.
Processors	Includes information regarding the processor of a target machine, such as vendor name and processor speed.
Motherboard	Includes information regarding the motherboard of a target machine, such as product name, manufacturer, version and serial number.
Memory details	Includes information regarding the memory allocation of a target machine, such as free physical/virtual memory available.
Storage details	Includes information regarding the storage of a target machine, such as floppy disk drive, CD/ROM and hard drives.
Display adapters	Includes information regarding the display and video devices of a target machine, such as the device manufacturer.
Other devices	Includes information of devices that does not fall under the mentioned categories above, such as keyboard, ports, mouse and human interface devices.

Software

Click **Software** to view all details involved in the software audit. The software audit amongst others displays information such as:

- Application name
- Publisher
- Version.

The table below describes the hardware information groups:

Table 45: Software information from an audit

Icon	Description
General Applications	Enumerates installed software on scan targets.
Antivirus Applications	Lists installed antivirus engines on scan targets.
Instant Messenger Applications	Lists all detected instances of Instant messenger applications on scan targets.
Patch Management Applications	Lists all the installed patch management applications, detected on your scan targets during a scan.
Web Browser Applications	Contains scanned targets that have Internet browsers installed.
Firewall Applications	Enumerates information on installed Firewall applications on scan targets.
Anti-phishing Applications	Lists information of installed anti-phishing engines on scan targets.
VPN Client Applications	Includes information on installed Virtual Private Network clients on scan targets.
Peer-To-Peer Applications	Shows installed Peer-To-Peer applications on scan targets.

System Information

Click **System Information** to view all details related to the operating system installed on a target machine. Table below describes the system information groups:

Table 46: System information from an audit

Category	Information	Identify
Shares	» Share name » Share remark (extra details on the share). » Folder which is being shared on the target computer » Share permissions and access rights » NTFS permissions and access rights.	» Users sharing entire hard-drives, shares that have weak or incorrectly configured access permissions. » Start-up folders, and similar system files, that are accessible by unauthorized users, or through user accounts, that do not have administrator privileges, but are allowed to execute code on target computers. » Unnecessary or unused shares.
Password Policy	» Minimum password length » Maximum password length » Minimum password expiry date » Force logoff » Password history.	» Incorrectly configured lockout control » Password strength enforcement policies.
Security Audit Policy	» Audit account logon events » Audit account management » Audit directory service access » Audit logon events » And more…	» Security holes or breaches. **Note** To view Security Audit Policy, enable auditing on target computers. For more information, refer to Manual scans (page 66).

Category	Information	Identify
Registry	» Registered owner » Registered organization » Product name » Current build number.	» Hardware and software settings such as which drivers and applications will be automatically launched at system startup.
NETBIOS Names	» Workstation service » Domain name » Domain controllers » File server service.	» Rogue computers » Wrong configurations.
Groups	» Account operators » Administrators » Backup operations » Guest.	» Wrong configurations » Security flaws due to rogue or obsolete user groups.
Users	» Full name » Privilege » Flags » Login.	» Rogue, obsolete or default user accounts.
Logged On Users	» List of logged on users.	» Authorized and unauthorized users currently logged on computers.
Sessions	» Lists hosts remotely connected to the target computer during scanning.	» Authorized and unauthorized remote connections.
Services	» List of active services.	» Rogue or malicious processes; redundant services.
Processes	» List of active processes.	» Rogue or malicious processes.
Remote TOD (time of day)	» Time of remote workstation, server or laptop.	» Time inconsistencies and regional settings » Wrong configurations.

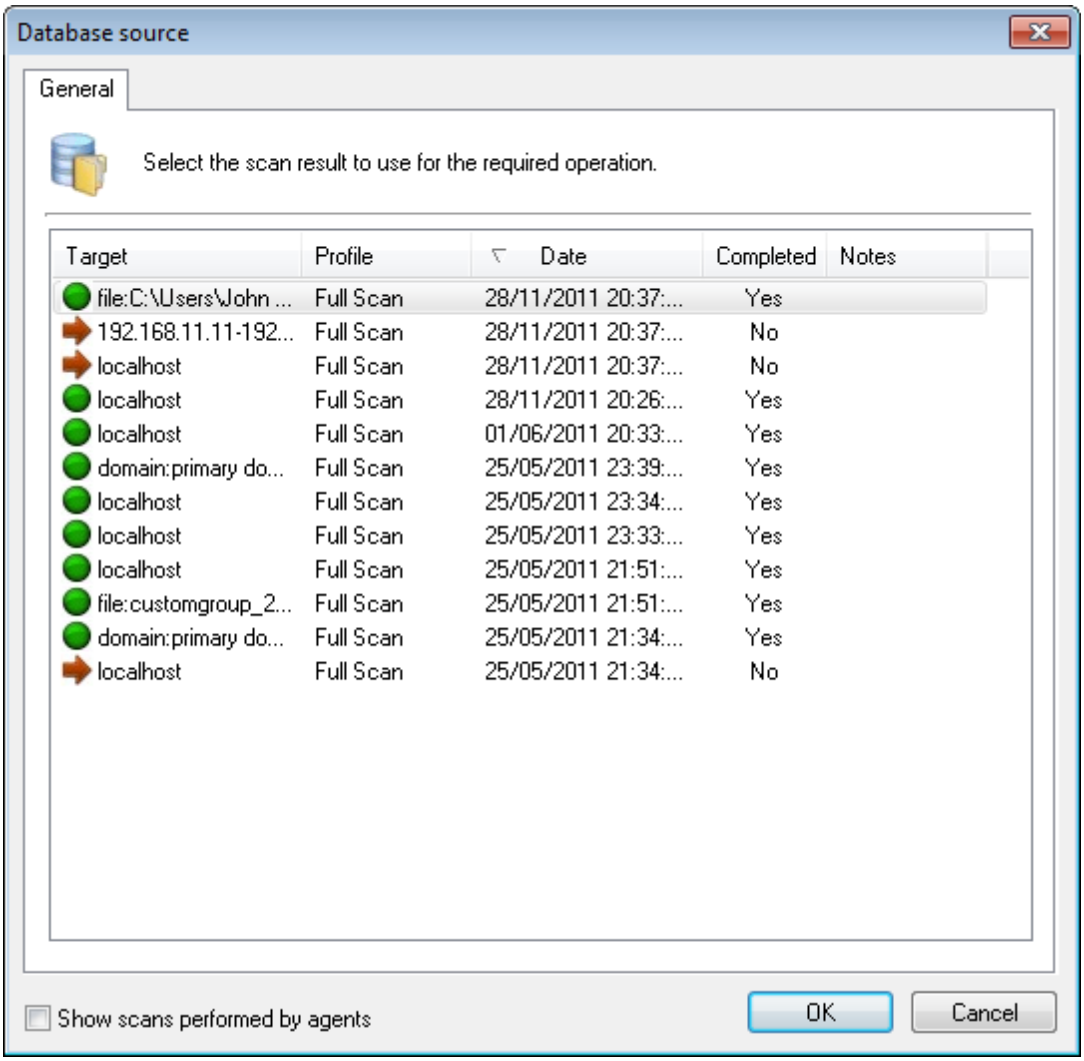
7.2 Loading results from the database

By default, saved scan results are stored in a database. GFI LanGuard stores the results data of the last 10 scans performed per scanning profile. You can configure the number of scan results that are stored in a database file. For more information, refer to Configuring Database Maintenance Options (page 178).

To load saved scan results from the database backend or from XML files:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button > **File > Load Scan Results from > Database...**



Screenshot 70: Reloaded scan results

3. Select the saved scan result and click **OK**.

4. Analyze loaded results. For more information on how to interpret results. refer to the following sections:

- Vulnerability Assessment
- Network and Software Audit.

7.3 Saving and loading XML results

Scan results are an invaluable source of information for systems administrators. GFI LanGuard results are stored in a SQL Server® or a Access™ database. In addition, scan results can also be exported to XML.

To save scan results to XML file:

1. Launch GFI LanGuard.

2. Perform a manual scan. For more information, refer to Manual scans (page 66).

3. Once the scan is completed, click GFI LanGuard button **> File > Save Scan Results**.

4. Locate the destination where you want to save the XML and click **Save**.

To load saved scan results from an XML file:

1. Click the GFI LanGuard button **> File > Load Scan Results from > XML File…**

2. Locate the scan results to load and click **OK**.

3. Analyze loaded results.

> **Note**
>
> For more information on how to interpret results, refer to the following sections:
>
> - Vulnerability Assessment
> - Network and Software Audit

8 Remediate Vulnerabilities

GFI LanGuard enables you to manually or automatically fix vulnerabilities on network computers. Use the information in this chapter to learn how to configure and manage remediation operations to maintain a high level of security amongst your scan targets.

Topics in this chapter:

8.1 Automatic Remediation 116

8.2 Manual Remediation 138

8.1 Automatic Remediation

Automatic-Remediation enables you to automatically download and deploy missing patches as well as uninstall unauthorized applications during scheduled operations, automatically.

> **IMPORTANT**
>
> Auto-remediation and un-installation of un-authorized applications only work with scanning profiles that detect missing patches and/or installed applications.

Automatic Remediation tasks:

- Review Auto-Remediation Considerations
- Configure Missing Updates Auto-Deployment
- Configure Unauthorized Applications Auto-Uninstall
- Configure Auto-Remediation options
- Configure Wake-on-LAN on client machines
- Configure End-User reboot and shut down options
- Define Auto-Remediation Messages
- Configure Agents Auto-remediation

8.1.1 Auto-remediation notes

Before enabling and configuring auto-remediation options, review the following notes about:

- Installing software
- Uninstalling software

Installing software

Always test patches in a test environment before deployment.

By default, Microsoft® updates are not enabled for automatic deployment. Manually approve each patch (as it is tested) or set all Microsoft® updates as approved.

Uninstalling software

To uninstall software, a 3-stage process is required in order to identify whether the selected application supports silent uninstall:

Table 47: Automatic remediation stages

Stage	Description
Stage 1	Select the application to auto-uninstall.
Stage 2	Ensure that application supports silent uninstall. Test this by trying to remotely uninstall the application. This is the validation process.
Stage 3	Setup a scheduled audit that will remove the unauthorized application. This is done automatically (using agents) or manually (agent-less approach).

Auto-remediation and un-installation of un-authorized applications only work with scanning profiles that detect missing patches and/or installed applications.

8.1.2 Configuring missing updates auto-deployment

GFI LanGuard ships with a patch auto-deployment feature, that enables you to automatically deploy missing patches and service packs in all 38 languages supported by Microsoft® products. GFI LanGuard also supports patching of third party (Non-Microsoft®) patches. For a complete list of supported third party applications visit refer to http://go.gfi.com/?pageid=3p_fullreport. Refer to the following section for information about:

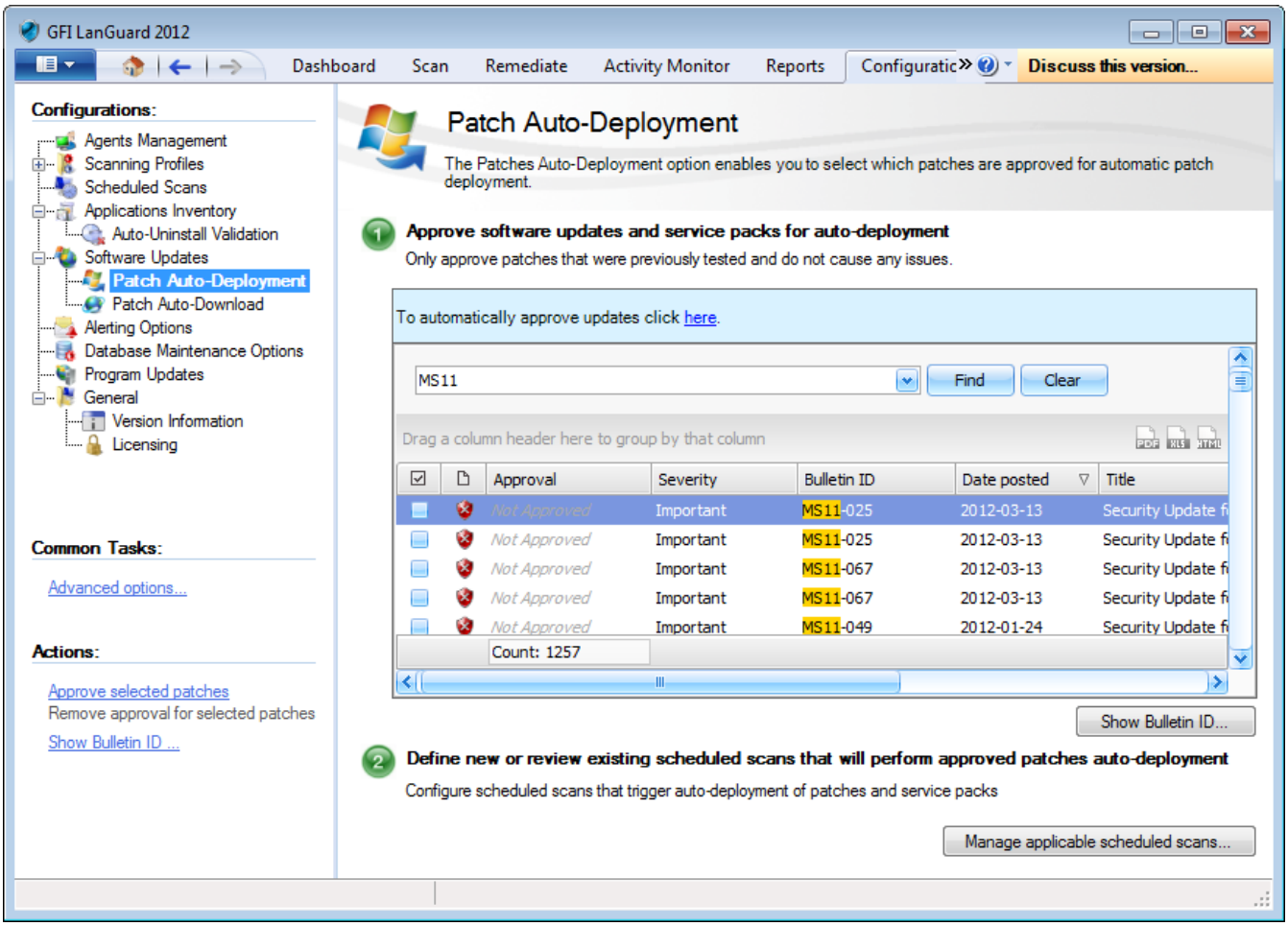
- Enabling Patch Auto-Deployment
- Configuring Patch Auto-Deployment advanced options
- Configuring Patch Auto-download settings

Enabling Patch Auto-Deployment

To configure patch auto-deployment:

1. Click on the **Configuration** tab > **Software Updates** > **Patch Auto-Deployment**.

2. In the right pane, select the patches to auto-deploy.



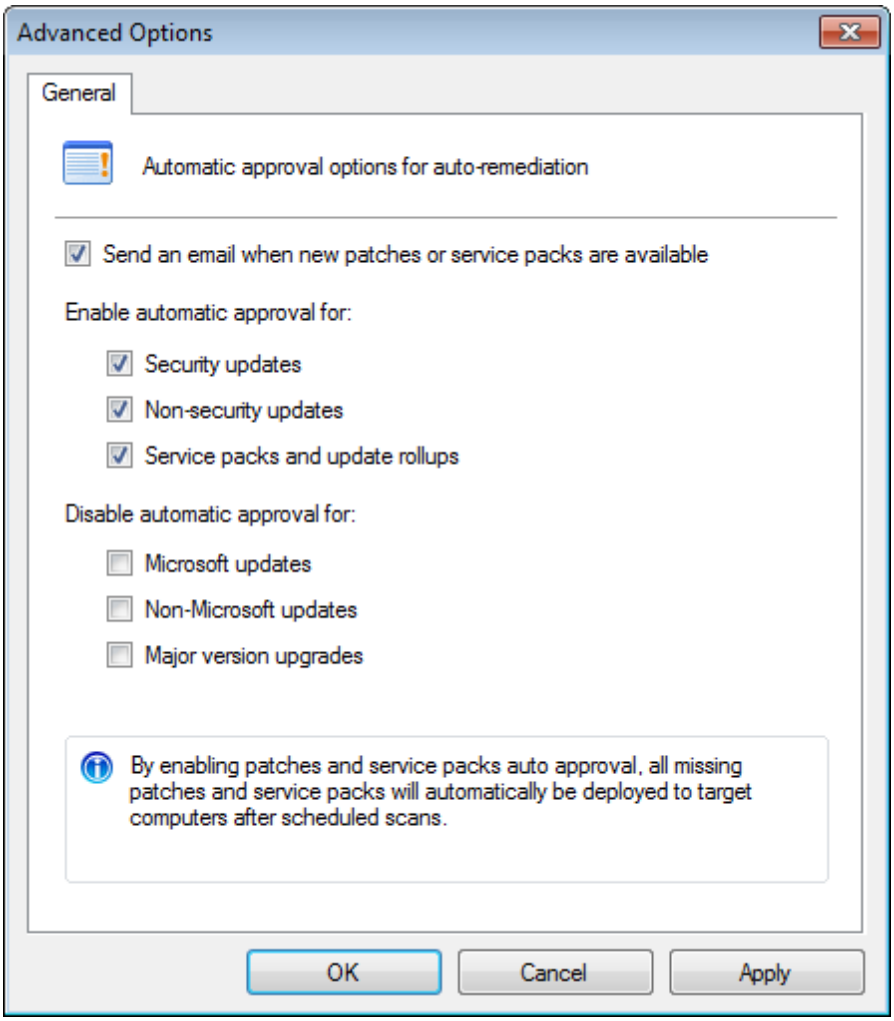
Screenshot 71: Patch auto-deployment

> **Note**
>
> Key-in a search criteria and click **Find** to search for a specific application.

Configuring Patch Auto-Deployment advanced options

To configure auto-remediation:

1. Click **Configuration** tab **> Software Updates > Patch Auto-Deployment** and from **Common Tasks**, click **Advanced options.**


Advanced Options
General
Automatic approval options for auto-remediation
Send an email when new patches or service packs are available
Enable automatic approval for:
Security updates
Non-security updates
Service packs and update rollups
Disable automatic approval for:
Microsoft updates
Non-Microsoft updates
Major version upgrades
By enabling patches and service packs auto approval, all missing patches and service packs will automatically be deployed to target computers after scheduled scans.
OK
Cancel
Apply

Screenshot 72: Patch Auto-Deployment Advanced Options

2. Configure the following options:

Table 48: Patch Auto-Deployment Advanced Options

Option	Description
Send an email when new patches or service packs are available.	Send an email when new patches are identified.
Enable automatic approval for:	Selected updates are automatically downloaded and installed on target computers. Select from the following: » Security updates » Non-security updates » Service packs and update rollups.
Disable automatic approval for	Selected updates are downloaded but not installed automatically on target computers. Select from the following: » Microsoft® updates » Non-Microsoft® updates » Major version upgrades. **Note** Updates can be installed manually from the **Remediation Center**. For more information, refer to Using the Remediation Center (page 138).

3. Select the appropriate check boxes and click **OK** to save changes.

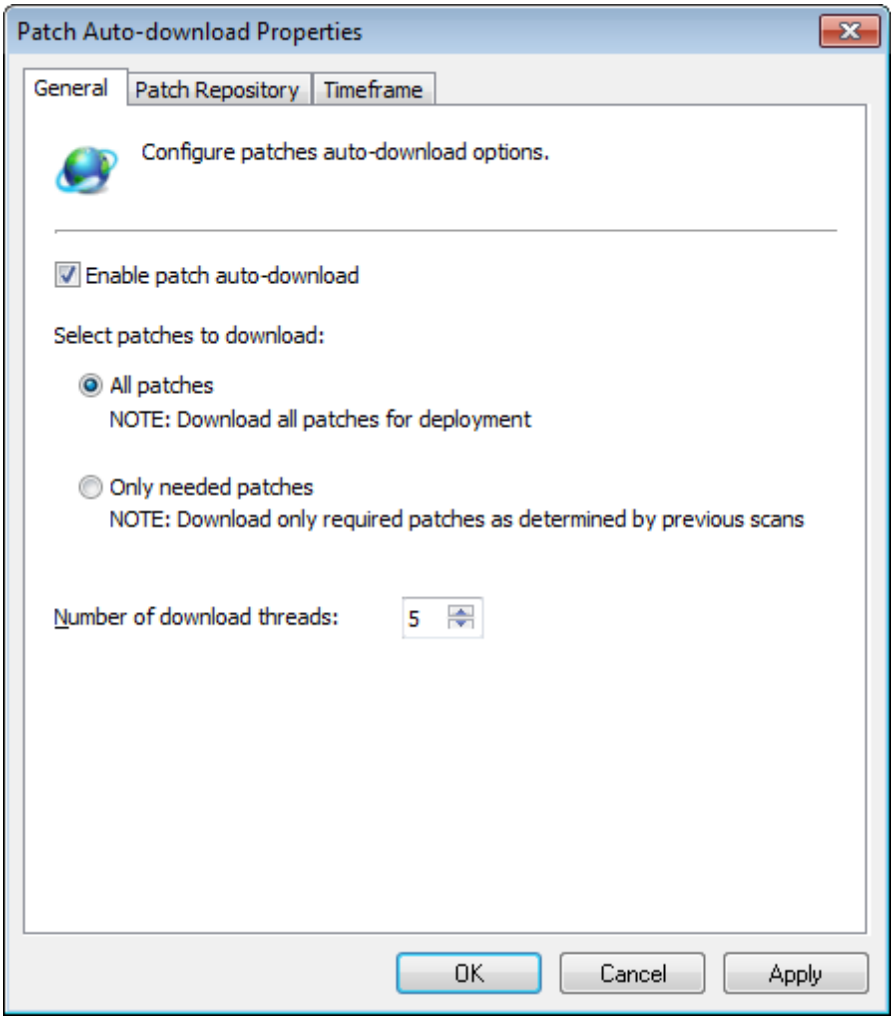
Configuring Patch Auto-download settings

GFI LanGuard ships with a patch auto-download feature, that enables the automatic download of missing patches and service packs in all 38 languages supported by Microsoft® products. In addition, you can also schedule patch auto-download by specifying the timeframe within which the download of patches is performed.

To configure patch auto-download:

1. Click **Configuration** tab > **Software Updates** > **Patch Auto-Download**.

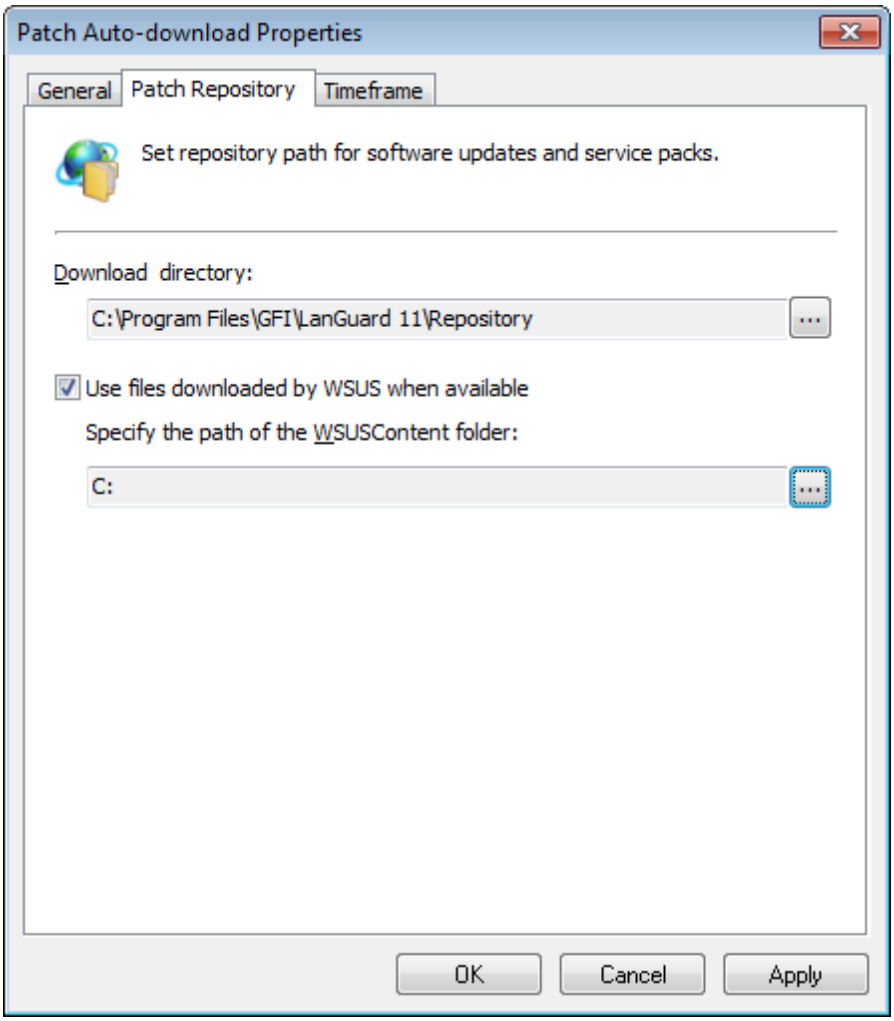
2. From the right pane, click the link.



Screenshot 73: Configuring Patch Auto-download Properties

3. In the **General** tab, select between **All patches** or **Only needed patches**.

> **Note**
>
> Selecting **All patches**, downloads all patches issued by Microsoft®, regardless of whether these are required for deployment. The Only needs patches option downloads only patches required for deployment.



Screenshot 74: Patch Repository settings

4. To change the location where the downloaded patches are stored click the **Patch Repository** tab and specify the required details.

5. Select **Use files downloaded by WSUS when available**, if you are using an existing setup of WSUS.

6. To change the timeframe during which patch downloads are performed, click **Timeframe** tab and specify the required details.

7. Click **Apply** and **OK**.

8.1.3 Configuring unauthorized applications auto-uninstall

Application auto-uninstall entails that applications marked as unauthorized for specific scanning profiles are first validated for a successful uninstall on a test machine. Subsequently a scheduled scan based on the scanning profile for which the application is marked as unauthorized, is configured to auto-uninstall applications.

GFI LanGuard applications inventory provides a list of all applications detected during past scans. The list is used to specify unauthorized applications. You can also manually add applications to the list. You can do this by specifying the entire name as well as a partial name, specify generic names or part of an application name. GFI LanGuard automatically scans the list of applications and detects partial names. Refer to the following sections for information about:

- Setting an application as unauthorized
- Adding new applications to the unauthorized list

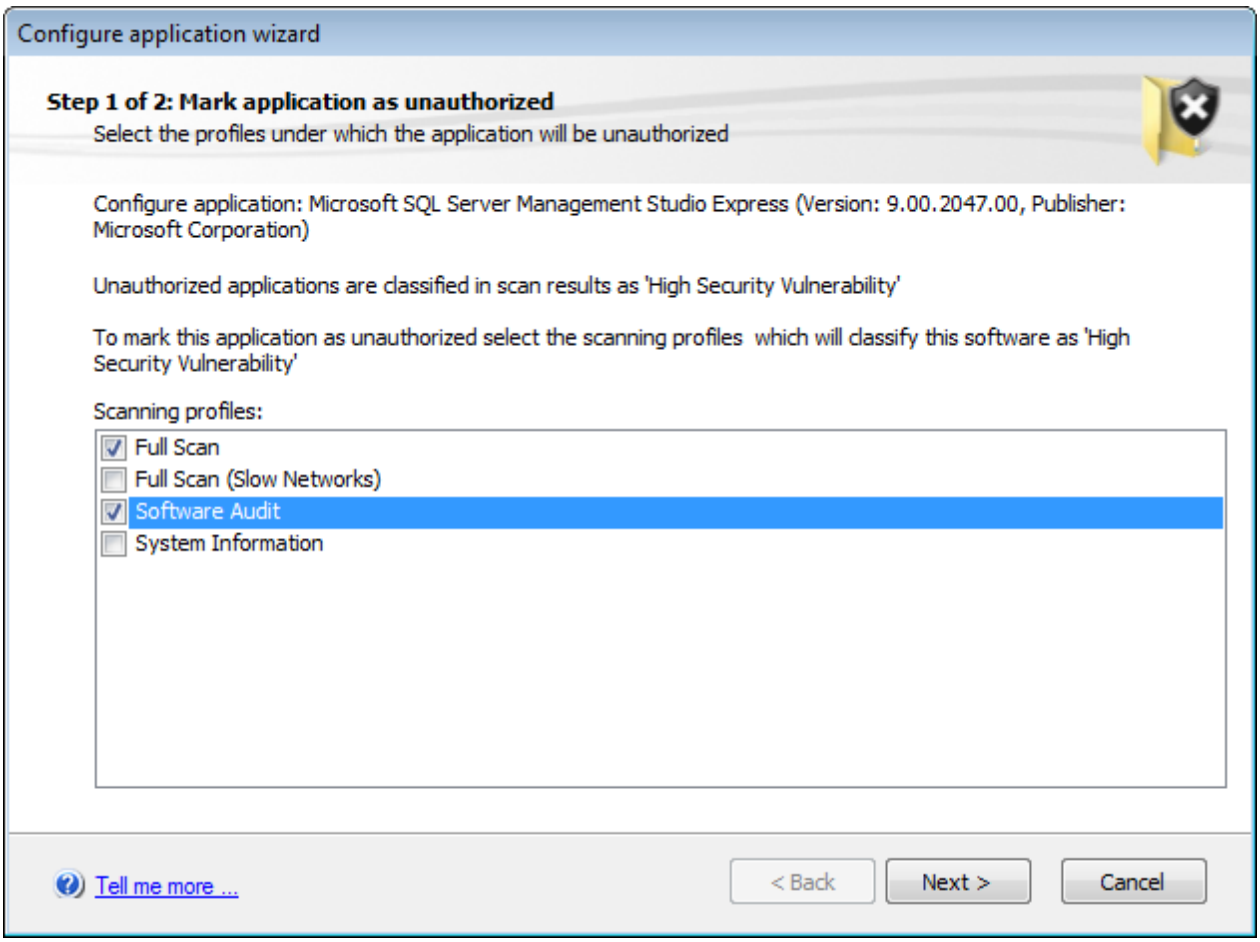
» Validating unauthorized applications for auto-uninstall

» Managing applicable scheduled scans

Setting an application as unauthorized

1. Click on **Configuration** tab > **Applications inventory** sub-node.

2. From the list of applications detected on the right, double click the application to set as unauthorized.


Configure application wizard
Step 1 of 2: Mark application as unauthorized
Select the profiles under which the application will be unauthorized
Configure application: Microsoft SQL Server Management Studio Express (Version: 9.00.2047.00, Publisher: Microsoft Corporation)
Unauthorized applications are classified in scan results as 'High Security Vulnerability'
To mark this application as unauthorized select the scanning profiles which will classify this software as 'High Security Vulnerability'
Scanning profiles:
Full Scan
Full Scan (Slow Networks)
Software Audit
System Information
Tell me more ...
< Back
Next >
Cancel

Screenshot 75: Unauthorized application

3. Select the scanning profile for which this application will be set as unauthorized and click **Next**.

4.GFI LanGuard can associate partial names with entries already in the list. As a result, the system will prompt you to confirm whether to apply the same changes also to applications partially have the same name.

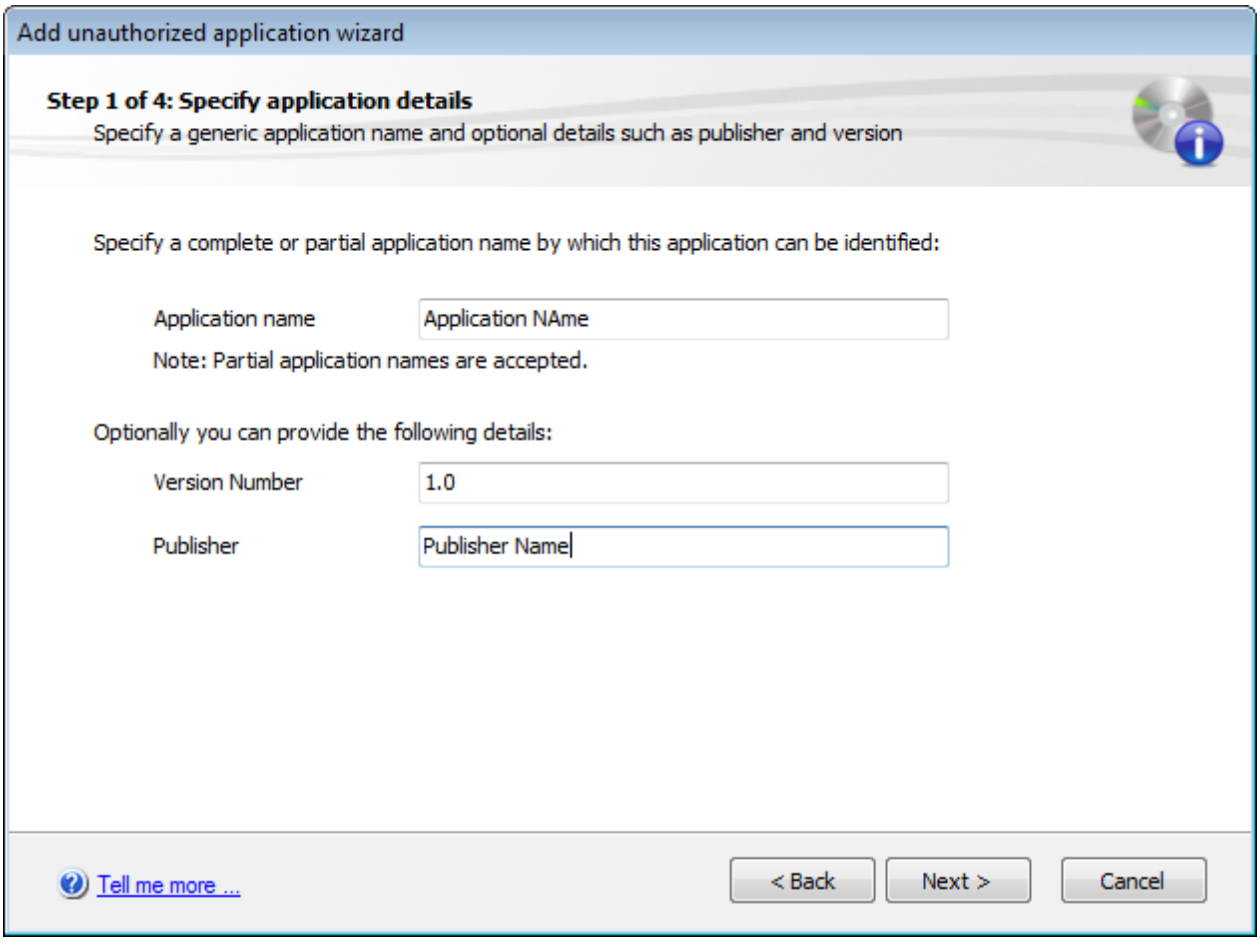
5. Click **Finish** to finalize settings.

Adding new applications to the unauthorized list

1. Click **Configuration** tab > **Applications inventory** sub-node.

2. From **Common Tasks**, click **Add a new application**.

3. In the welcome screen, click **Next**.


Add unauthorized application wizard
Step 1 of 4: Specify application details
Specify a generic application name and optional details such as publisher and version
Specify a complete or partial application name by which this application can be identified:
Application name
Application NAme
Note: Partial application names are accepted.
Optionally you can provide the following details:
Version Number
1.0
Publisher
Publisher Name
Tell me more ...
< Back
Next >
Cancel

Screenshot 76: Applications inventory wizard

4. Specify application name. Optionally provide the version number and publisher name. Click **Next**.

5. Select the scanning profiles that will detect unauthorized applications (Example: Full Scan) and click **Next**.

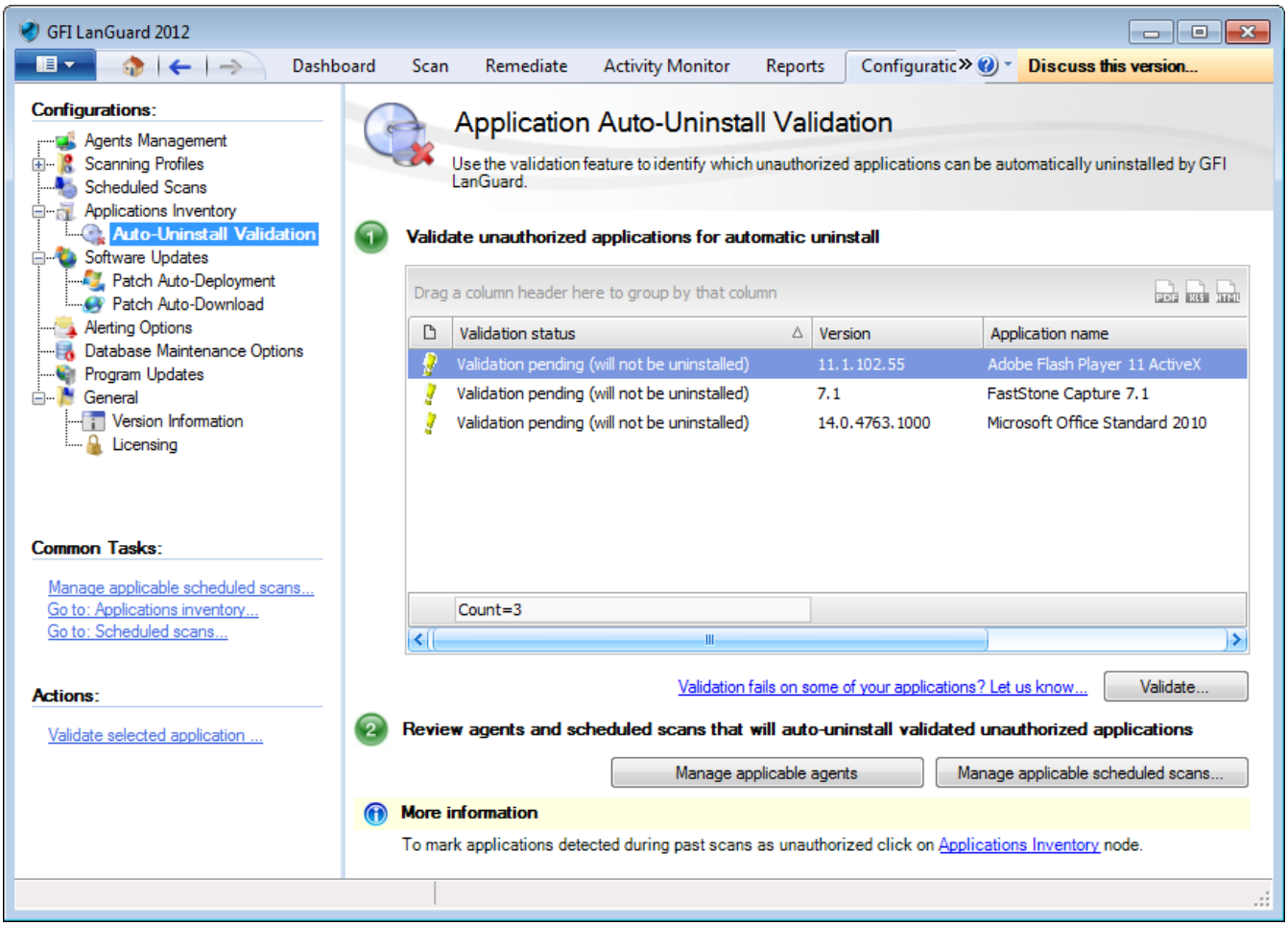
6. Specify whether changes made will effect applications, which have partial/full name match. Click **Next** to continue.

7. Review the information and click **Finish**.

Validating unauthorized applications for auto-uninstall

Application auto-uninstall validation enables you to validate the uninstallation procedure for the applications which are to be automatically uninstalled by GFI LanGuard. This is a requirement prior to the actual uninstallation process and no applications are un-installed during scans unless verified.

1. Click **Configuration** tab > **Applications Inventory** > **Auto-Uninstall Validation**



Screenshot 77: Application auto-uninstall validation

2. From the right pane, select an application to validate and click **Validate**.
3. In the **Application auto-uninstall validation** wizard, click **Next**.
4. Select the computer where to test the application auto-uninstall and click **Next**.
5. Provide the authentication details for the validation operation and click **Next**.
6. Review the Auto-uninstall validation wizard information and click **Start**.

Managing applicable scheduled scans

The **Manage applicable scheduled scans** button enables you to review or edit scheduled scans, which will perform the validated applications auto install. To manage a scheduled scan:

1. From the **Auto-Uninstall validation** pane, click **Manage applicable scheduled scans**.
2. From, **Manage applicable schedule scans** dialog, click one of the options described below:

Table 49: Manage applicable schedule scans

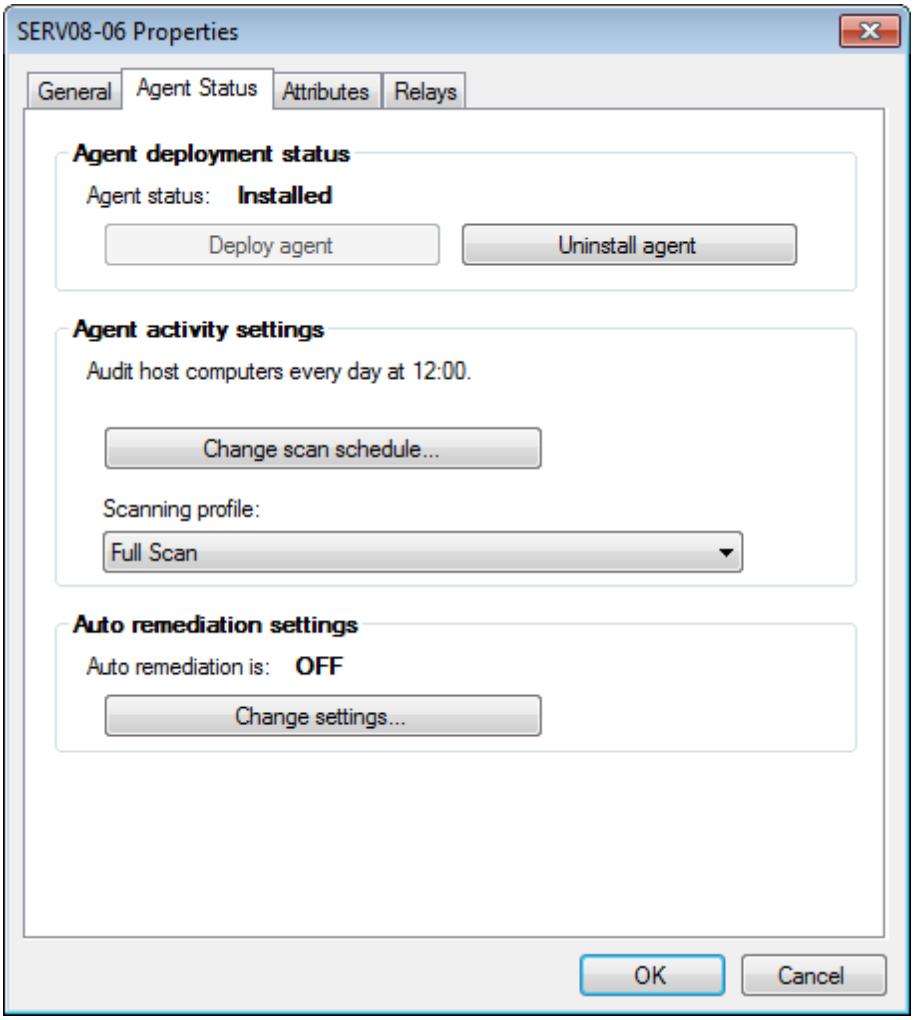
Option	Description
Edit selected scan...	Modify the selected schedule scan. For more information, refer to Editing scheduled scan settings (page 79).
Create a new scheduled scan...	Add a new scheduled scan using the new scheduled scan wizard. For more information, refer to Creating a scheduled scan (page 71).
View all scheduled scans...	Manage scheduled scans. For more information, refer to Editing scheduled scan settings (page 79).

8.1.4 Configuring auto-remediation options

To edit the general deployment options:

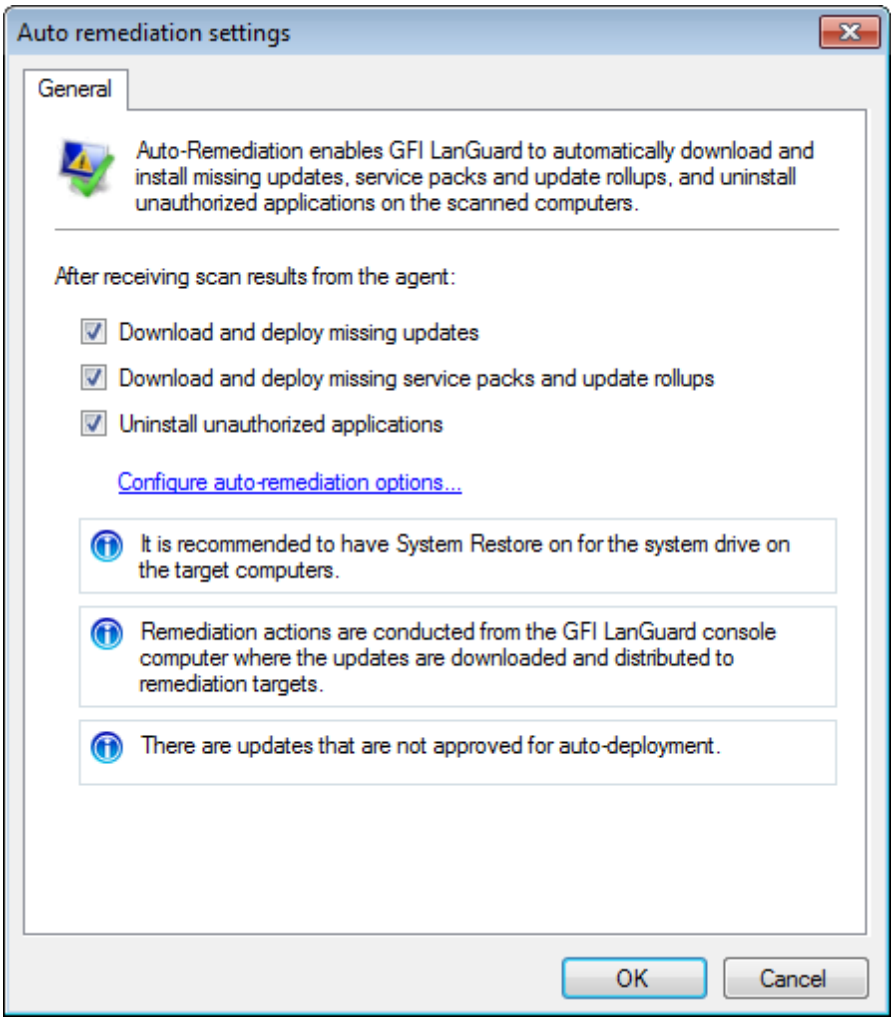
1. Launch GFI LanGuard.

2. From the computer tree, right-click a computer/computer group and select **Properties**.



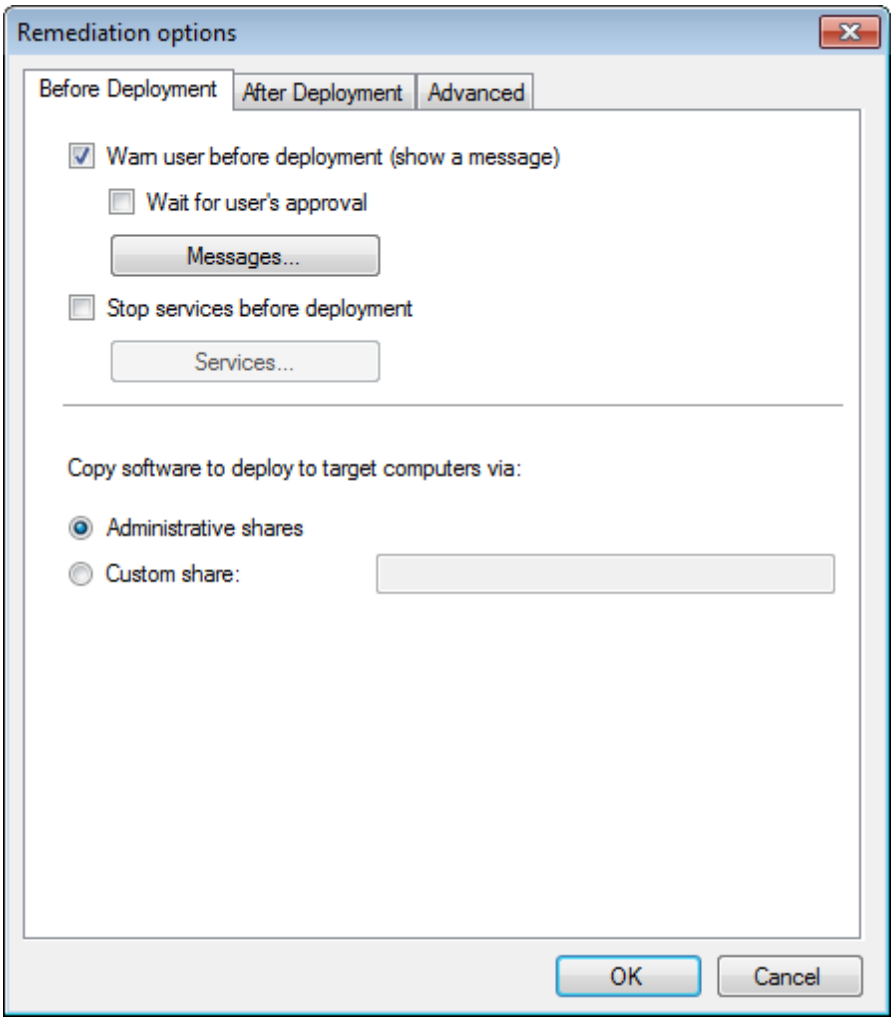
Screenshot 78: Computer properties

3. Select the **Agent Status** tab and from **Auto remediation settings**, click **Change settings...**


Auto remediation settings
General
Auto-Remediation enables GFI LanGuard to automatically download and install missing updates, service packs and update rollups, and uninstall unauthorized applications on the scanned computers.
After receiving scan results from the agent:
Download and deploy missing updates
Download and deploy missing service packs and update rollups
Uninstall unauthorized applications
Configure auto-remediation options...
It is recommended to have System Restore on for the system drive on the target computers.
Remediation actions are conducted from the GFI LanGuard console computer where the updates are downloaded and distributed to remediation targets.
There are updates that are not approved for auto-deployment.
OK
Cancel

Screenshot 79: General auto-remediation settings

4. Select the action to take after receiving scan results from the agent. Click **Configure auto-remediation options...**

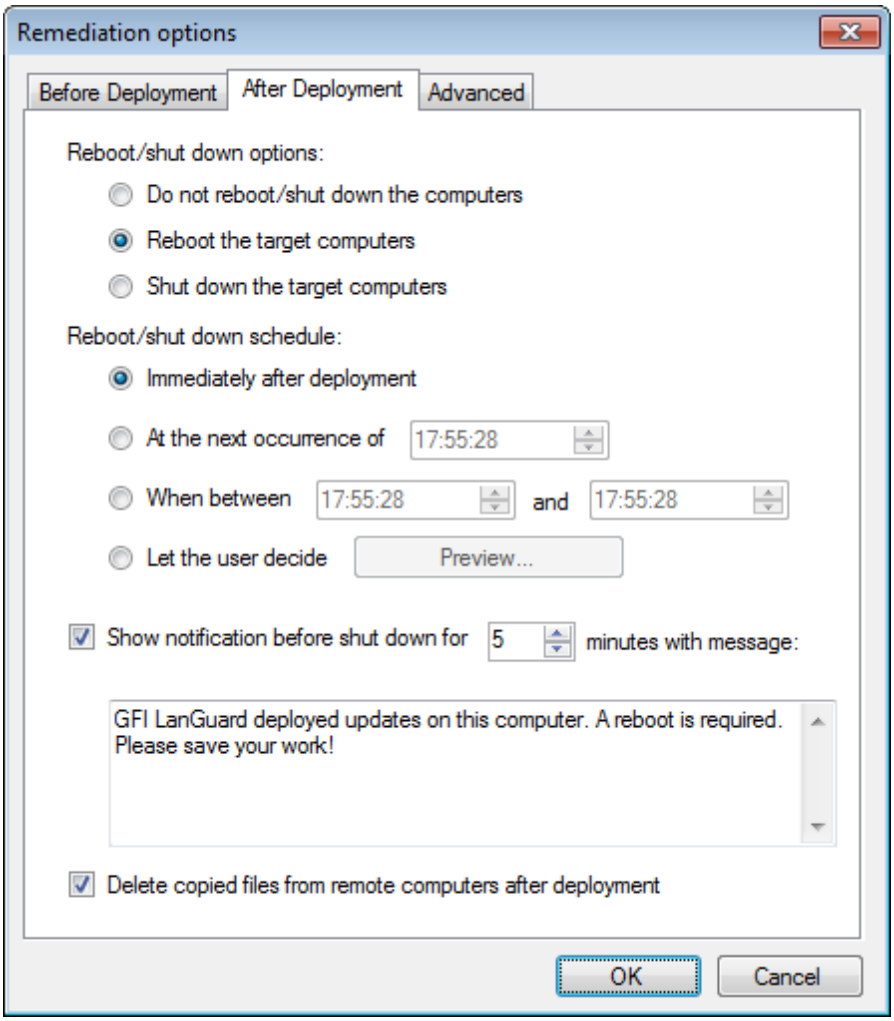


Screenshot 80: Before deployment options

5. Configure **Before Deployment** options described below:

Table 50: Before deployment

Option	Description
Wake up offline computers	Start computers if they are turned off. For more information, refer to Configuring Wake-on-LAN on scan targets (page 130).
Warn user before deployment (show message)	Displays a message on the target machine to warn the user before deploying software.
Wait for user's approval	Wait for user's approval Waits for user approval before deploying software.
Messages	Click **Messages** to select the end-user's computer language and define the warning message. For more information, refer to Configuring auto-remediation messages (page 132).
Administrative shares	Make a copy of the software on the default network shares.
Custom shares	Make a copy of the software in a custom share. Key-in the folder name in the text box.
Remember settings	Saves your configured settings and uses them during the next remediation job.



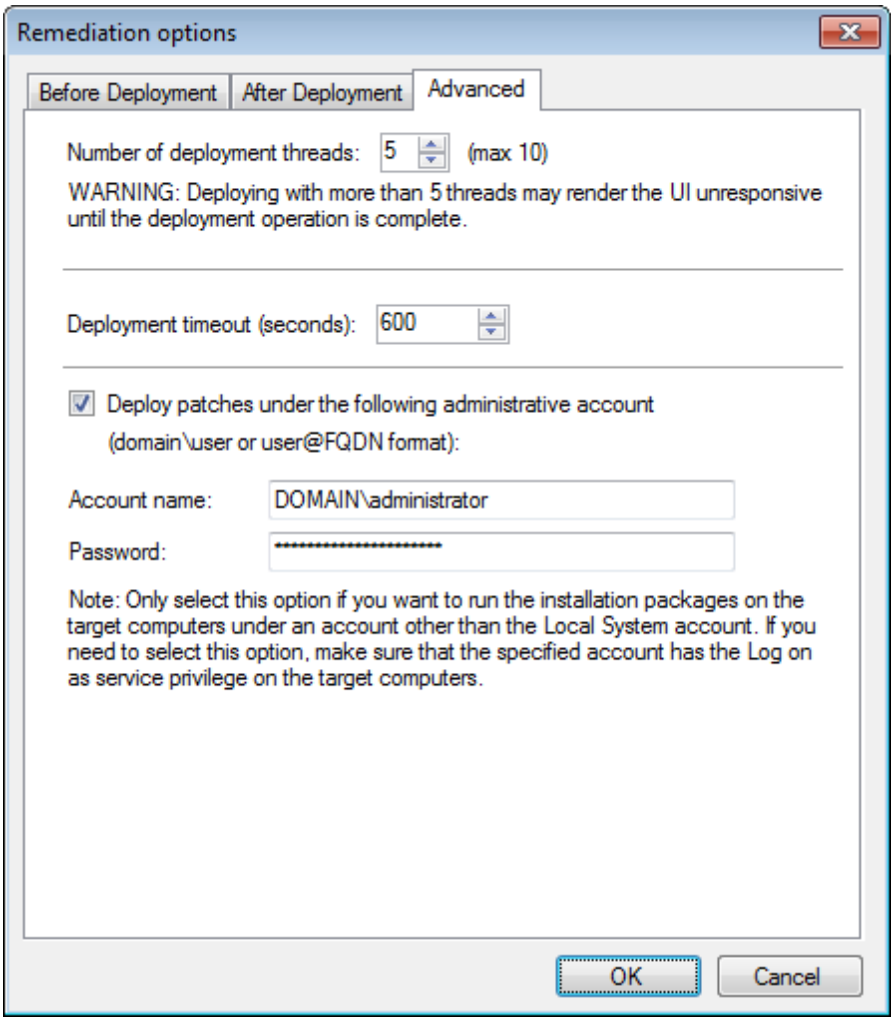
Screenshot 81: After deployment options

6. Click **After Deployment** tab. Configure **After Deployment** options described below:

Table 51: After deployment

Option	Description
Do not reboot/shut-down the computer	Select this option to leave scan target(s) turned on after remediating vulnerabilities.
Reboot the target computers	Reboots the computers after remediating vulnerabilities.
Shut down the target computers	Target machine will shut down after deploying software.
Immediately after deployment	Reboots/shuts down computers immediately after remediating vulnerabilities.
At the next occurrence of	Specify the time when the computers reboot/shut down.
When between	This option enables you to specify two time values. If the remediation job is completed between the specified times, the computer(s) will reboot/shut down immediately. Otherwise, the reboot/shut down operation is postponed until the next entrance into the specified time interval.
Let the user decide	Click **Preview** to view a screenshot of the dialog in the user manual. This dialog opens on the end-user's computer after remediating vulnerabilities. For more information, refer to Configuring end-user reboot and shut down options (page 132).
Show notification before shut down for	Shows a custom message on the end user's computer for a specified number of minutes before reboot/shut down.

Option	Description
Delete copied files from remote computers after deployment	Deletes the downloaded patches / service packs after they are deployed.
Remember settings	Saves your configured settings and uses them during the next remediation job.


Remediation options
Before Deployment
After Deployment
Advanced
Number of deployment threads:
5
(max 10)
WARNING: Deploying with more than 5 threads may render the UI unresponsive until the deployment operation is complete.
Deployment timeout (seconds):
600
Deploy patches under the following administrative account
(domain\user or user@FQDN format):
Account name:
DOMAIN\administrator
Password:
Note: Only select this option if you want to run the installation packages on the target computers under an account other than the Local System account. If you need to select this option, make sure that the specified account has the Log on as service privilege on the target computers.
OK
Cancel

Screenshot 82: Advanced deployment options

7. (Optional) Select **Advanced** tab. Configure the options described below:

Table 52: Advanced deployment options

Option	Description
Number of deployment threads	Specify the maximum number of processing threads allowed to start when deploying software updates. The number of threads determines the number of concurrent deployment operations an agent can handle.
Deployment timeout (seconds)	Specify the time (in seconds) an agent attempts to deploy an update. If the specified time is exceeded, the agent stops the unresponsive deployment and starts a new deployment thread. This feature enables you to stop the process thread so that if an update is taking longer than normal deployment time, the remediation operation continues without jeopardizing the rest.
Deploy patches under the following administrative account	Select this option to use a custom administrative account to log and deploy patches on target machines. The account selected must have Log-on as service privilege on the target computers. For more information on how to configure an account with log-on as service privilege, refer to http://go.gfi.com/?pageid=LAN_LogonService.

8. Click **OK** to apply changes.

Configuring Wake-on-LAN on scan targets

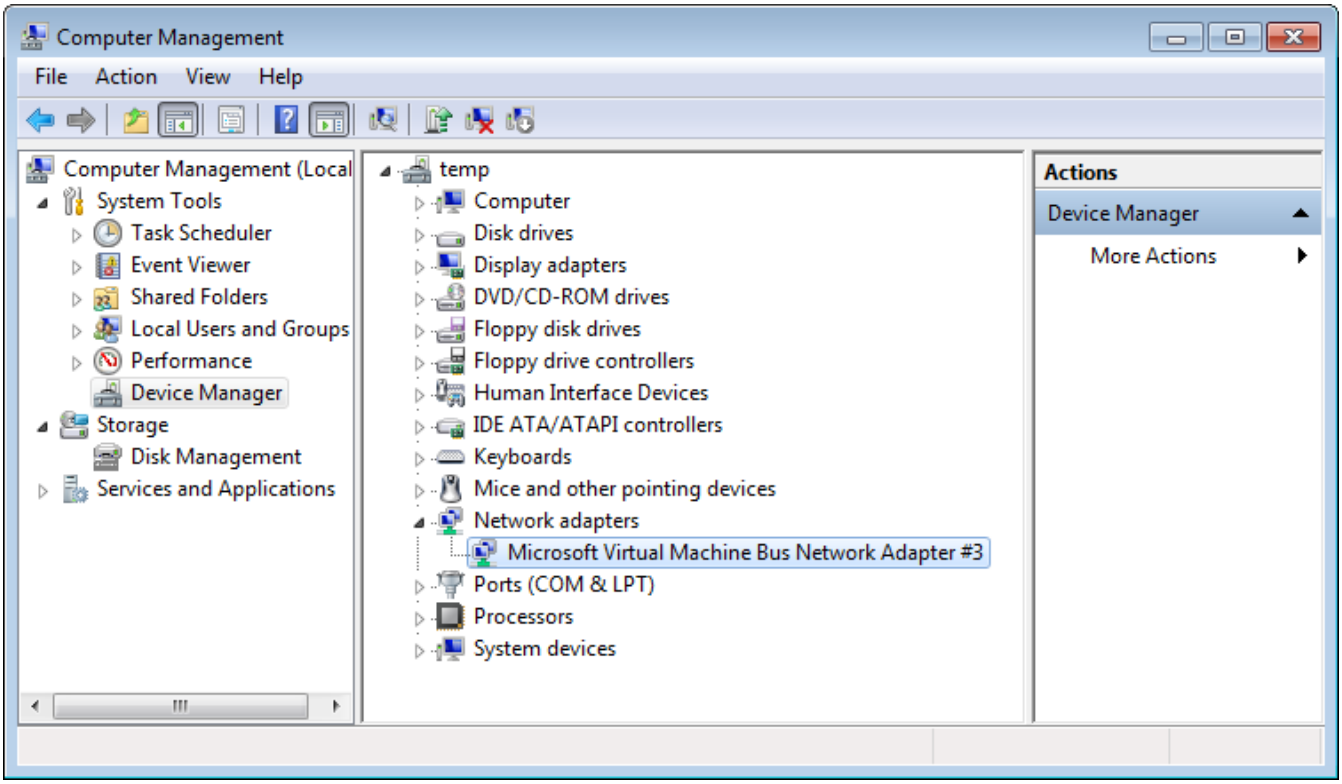
Wake-on-LAN enables GFI LanGuard to wake machines from the following states:

- Powered off
- Sleep
- Hibernated.

The motherboard and the network interface card of the computer running GFI LanGuard, must support Wake-on-LAN. To configure Wake-on-LAN on Windows® 7:

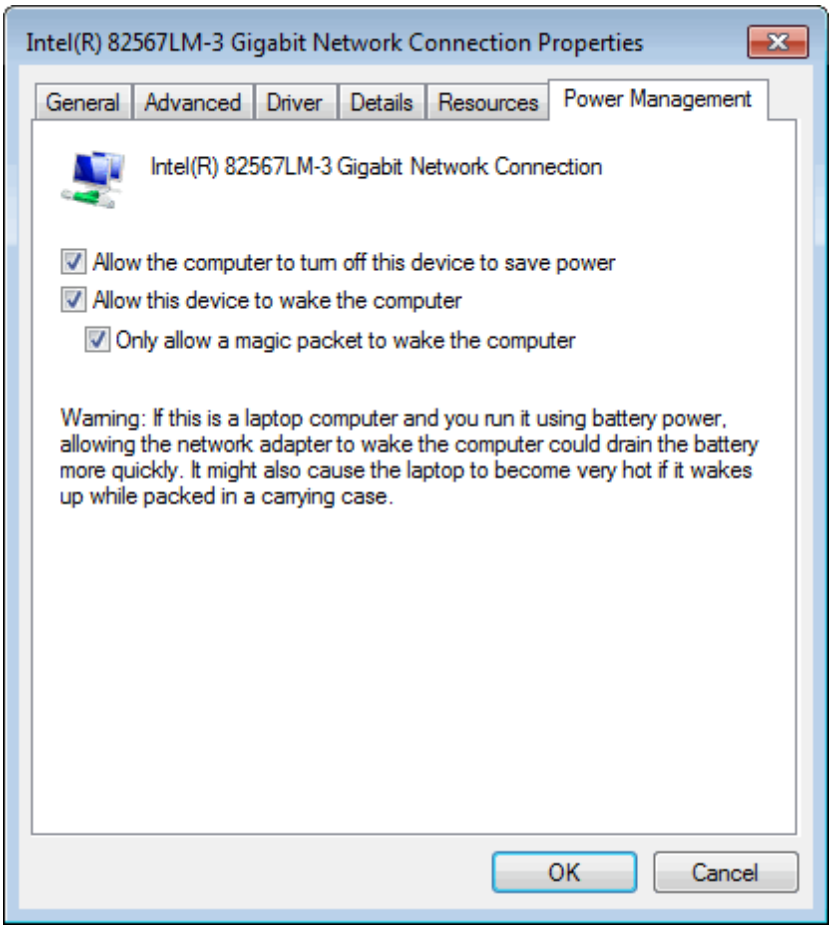
1. Click **Start**, right click **Computer** and select **Manage**.

2. From the left panel, expand **System Tools** and click **Device Manager**.



Screenshot 83: Device Manager

3. Right click the **Network Interface Card** and select **Properties**.


Intel(R) 82567LM-3 Gigabit Network Connection Properties
General
Advanced
Driver
Details
Resources
Power Management
Intel(R) 82567LM-3 Gigabit Network Connection
Allow the computer to turn off this device to save power
Allow this device to wake the computer
Only allow a magic packet to wake the computer
Warning: If this is a laptop computer and you run it using battery power, allowing the network adapter to wake the computer could drain the battery more quickly. It might also cause the laptop to become very hot if it wakes up while packed in a carrying case.
OK
Cancel

Screenshot 84: Power Management

4. From the **Power Management** tab, select the following options:

» **Allow this device to wake up the computer**

» **Only allow a magic packet to wake the computer**

> **Note**
>
> **Magic Packet** is the wake up signal that is sent by GFI LanGuard to the scan target network card.

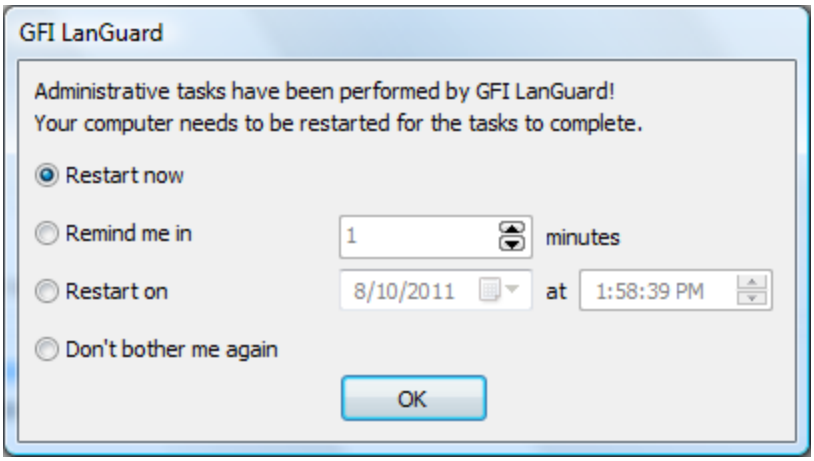
5. Click **OK**.

Once the **Network Interface Card** is configured, run a **FULL** scan on the client machine. This enables GFI LanGuard to gather the required information from the client machine. For more information, refer to Manual scans (page 66).

> **IMPORTANT**
>
> If you have routers between the client machine and the GFI LanGuard machine, the router and the GFI LanGuard machine must be configured to allow Wake-on-LAN broadcast packets on UDP port 9.

8.1.5 Configuring end-user reboot and shut down options

When configuring **After Deployment** settings, in **Auto-remediation options**, you can configure GFI LanGuard to notify and let the user decide when to reboot or shut down the computer after completing an administrative task. The below dialog opens on the user's computer and enables him/her to select one of the following options:



Screenshot 85: Reboot/shut down options

The table below describes the available options:

Table 53: Advanced deployment options

Option	Description
Restart now	Reboots/shuts down the computer immediately after completing an administrative task.
Remind me in	Specify a time interval (in minutes), when to remind the end-user.
Restart on	Specify the date and time when the machine reboots/shuts down.
Don't bother me again	The user is not prompted again.

8.1.6 Configuring auto-remediation messages

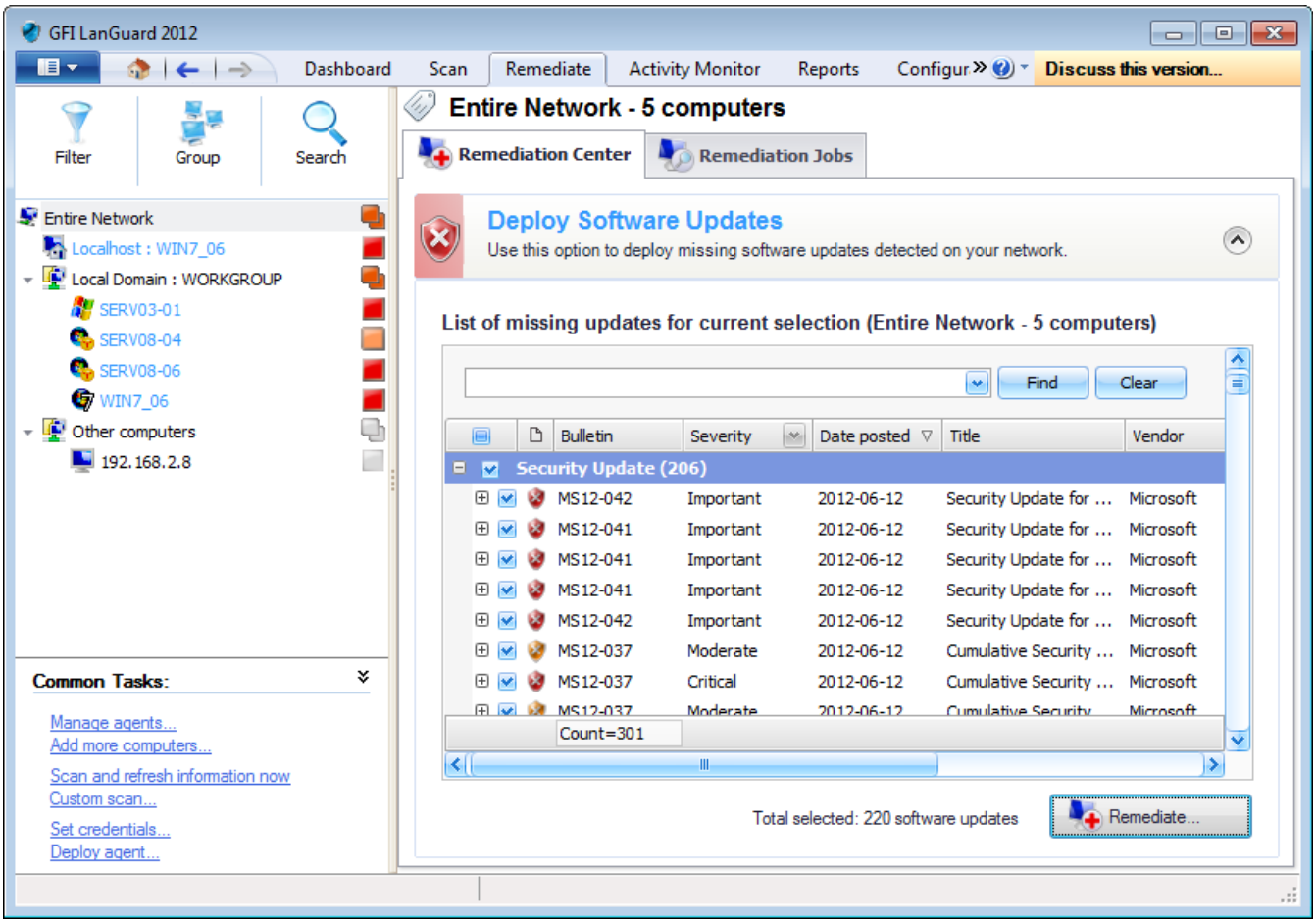
GFI LanGuard enables you to automatically display warning messages before and after remediation operations. These messages are displayed on the end-users' computer and in some cases, allows them to select after deployment options, or notify them about the operations to be carried out. You can customize predefined messages and set the language according to the scan target's computer language.

To configure warning messages:

1. Launch GFI LanGuard.

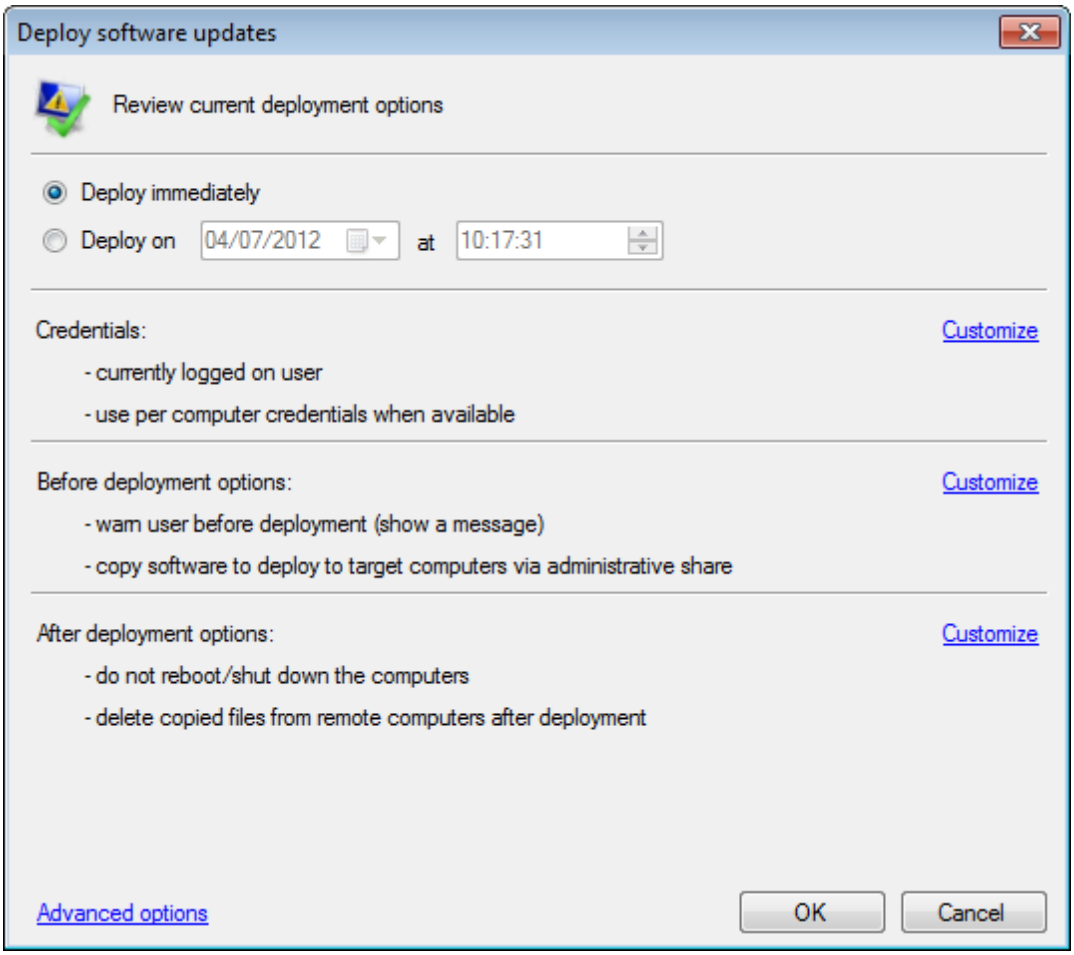
2. Click **Remediate tab > Remediation Center**.

3. From **Remediation Center**, select a remediation action, such as **Deploy Software Updates**.



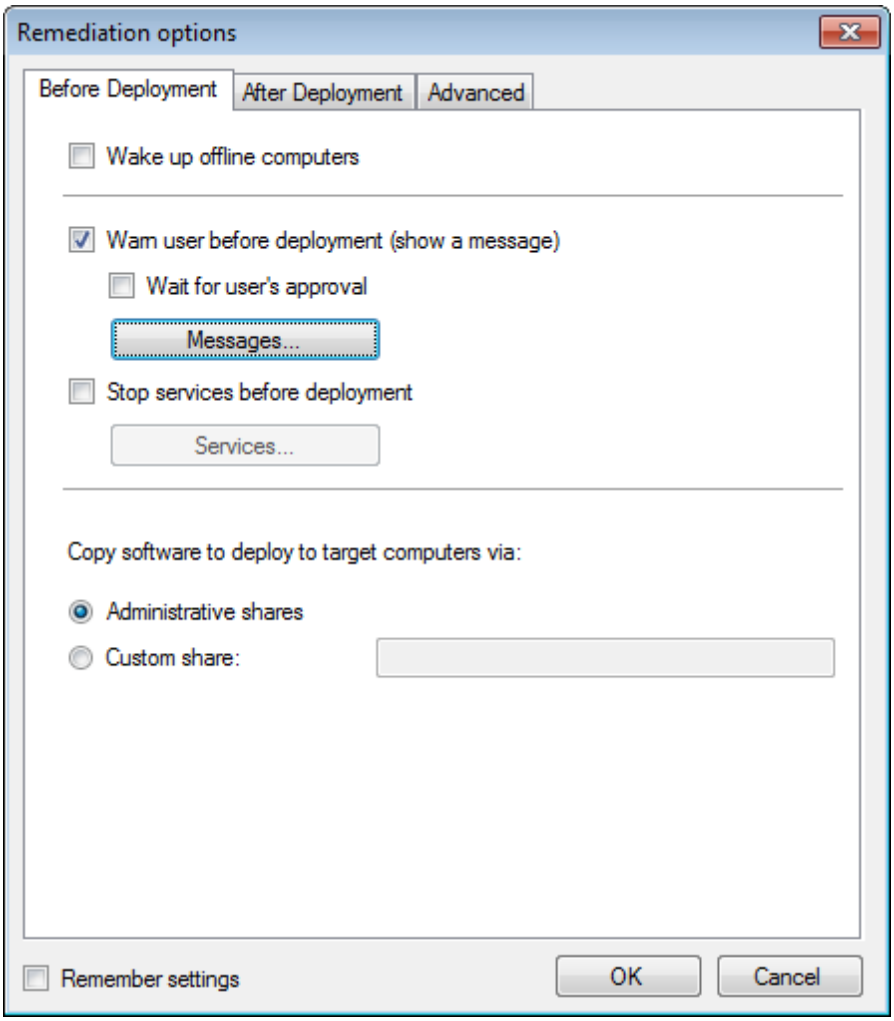
Screenshot 86: Remediation Center - Deploy Software Updates

4. Click **Remediate**.



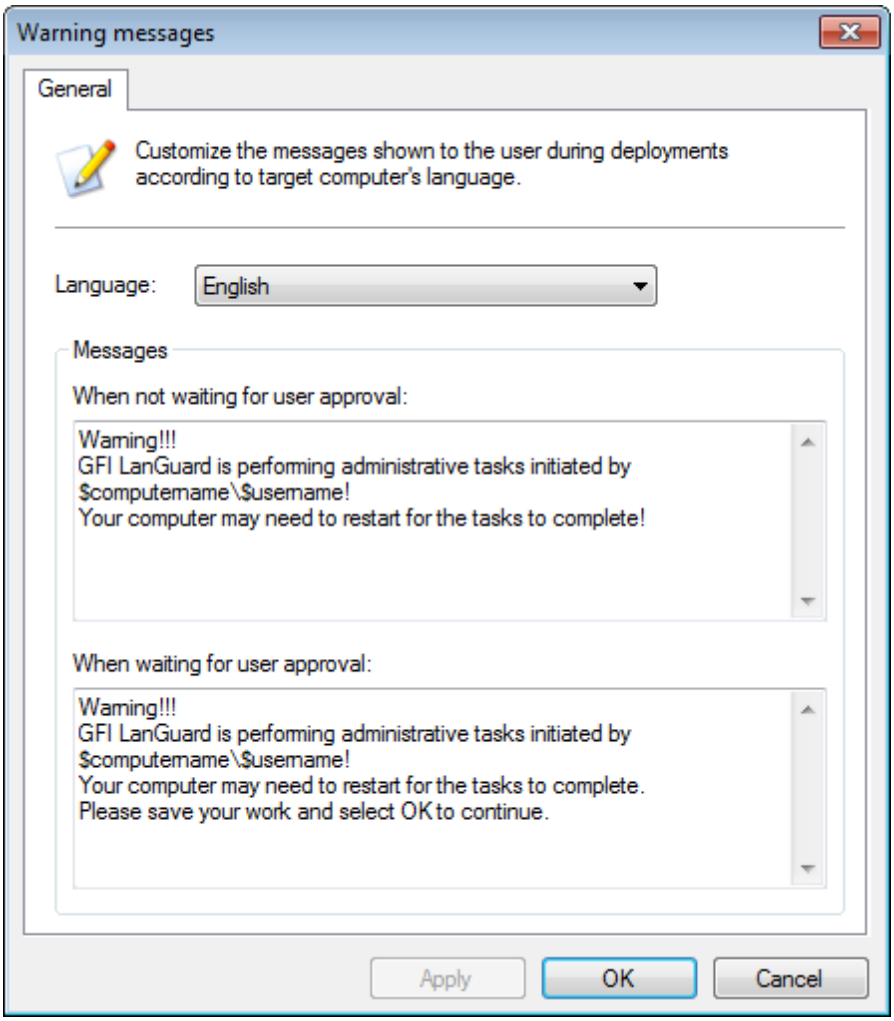
Screenshot 87: Deployment options dialog

5. Click **Advanced options.**



Screenshot 88: Before Deployment Message options

6. From the **Remediation options** dialog, click **Before Deployment tab > Messages...**.


Warning messages
General
Customize the messages shown to the user during deployments according to target computer's language.
Language:
English
Messages
When not waiting for user approval:
Warning!!!
GFI LanGuard is performing administrative tasks initiated by $computername\$username!
Your computer may need to restart for the tasks to complete!
When waiting for user approval:
Warning!!!
GFI LanGuard is performing administrative tasks initiated by $computername\$username!
Your computer may need to restart for the tasks to complete.
Please save your work and select OK to continue.
Apply
OK
Cancel

Screenshot 89: Customizing warning messages

7. Customize any of the following options:

Table 54: Warning messages

Option	Description
Language	Select the message language.
When not waiting for user approval	Use or customize the pre-defined message that launches on the end user's computer when GFI LanGuard is not waiting for approval.
When waiting for user approval	Use or customize the pre-defined message that launches on the end user's computer when GFI LanGuard is waiting for approval.

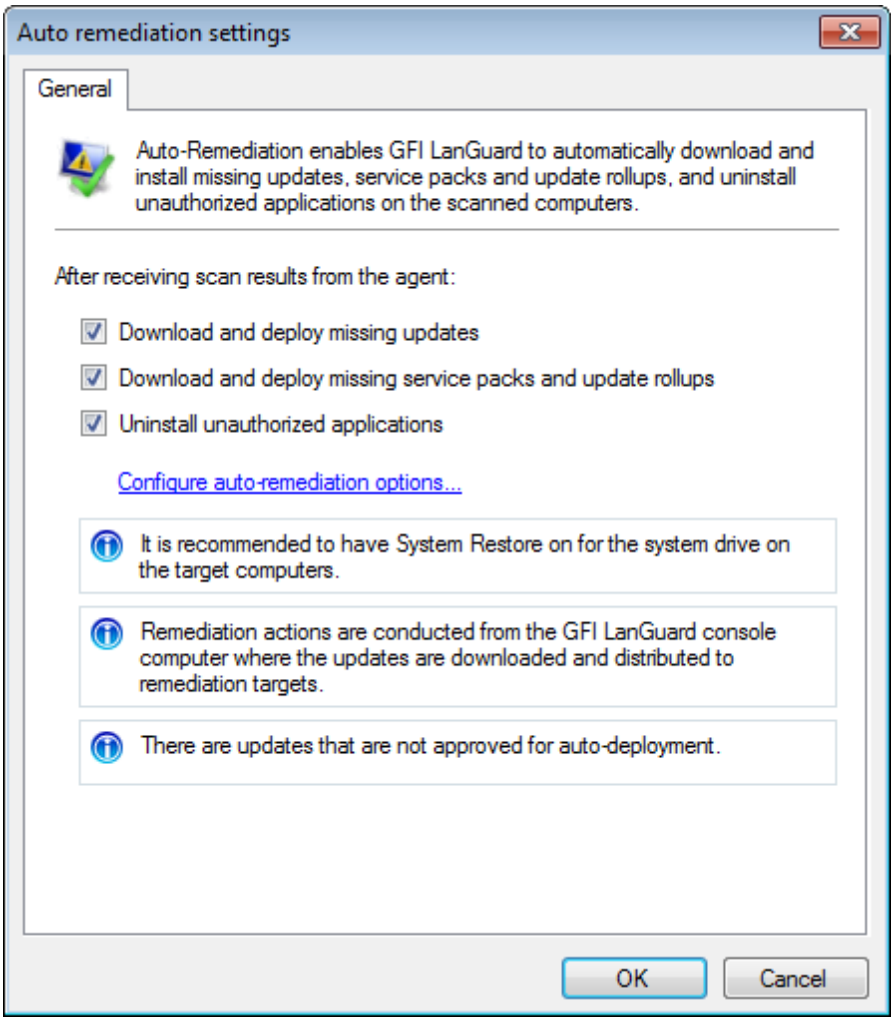
8. Click **Apply** and **OK**.

8.1.7 Configuring Agent auto-remediation

In an agent-based environment, automatic remediation options can be set for every deployed agent. This enables you to configure every agent with specific auto-remediation options to suit your requirements.

To configure agent auto-remediation actions:

1. Launch GFI LanGuard.
2. Click **Configuration** tab > **Agents Management**.
3. From the right pane, right-click an agent and select **Properties**.
4. Select the **Agent Status** tab and in the **Auto remediation settings** section click **Change Settings**.


Auto remediation settings
General
Auto-Remediation enables GFI LanGuard to automatically download and install missing updates, service packs and update rollups, and uninstall unauthorized applications on the scanned computers.
After receiving scan results from the agent:
Download and deploy missing updates
Download and deploy missing service packs and update rollups
Uninstall unauthorized applications
Configure auto-remediation options...
It is recommended to have System Restore on for the system drive on the target computers.
Remediation actions are conducted from the GFI LanGuard console computer where the updates are downloaded and distributed to remediation targets.
There are updates that are not approved for auto-deployment.
OK
Cancel

Screenshot 90: Agent auto-remediation

5. Select **Download and deploy missing updates** to enable automatic remediation for missing patches.

6. Select **Download and deploy missing service packs and update rollups** to enable automatic remediation for missing service packs.

7. Select **Uninstall unauthorized applications** to enable automatic remediation for unauthorized applications.

8. (Optional) Click **Configure auto-remediation options…** to further customize remediation options. For more information, refer to Configuring auto-remediation options (page 125).

9. Click **OK**.

8.2 Manual Remediation

Apart from automatically downloading patches and service packs, GFI LanGuard can also deploy these updates network-wide as well as recall any patches that were deployed.

Both patch deployment and patch rollback operations are managed by an agent service that manages all file transfers between GFI LanGuard and remote targets. This service is installed automatically on the remote target computer during the patch deployment process.

Manual Remediation tasks:

- Review Manual Remediation important notes
- Learn more about the Remediation Center
- Deploy Software Updates
- Uninstall Software Updates
- Deploy custom software
- Uninstall Applications
- Be protected against Malware
- Connect remotely to a machine using GFI LanGuard.

8.2.1 Manual remediation notes

1. While an infrequent occurrence, patches may be recalled due to newly discovered vulnerabilities or problems caused by the installation of these updates such as conflict issues with present software or hardware. Examples of updates recalled by the manufacturer include patches MS03-045 and MS03-047 for Exchange that were released by Microsoft® on October 15, 2006.

2. Ensure that the NetBIOS service is enabled on the remote target computer. For more information, refer to Configuring NetBIOS (page 243).

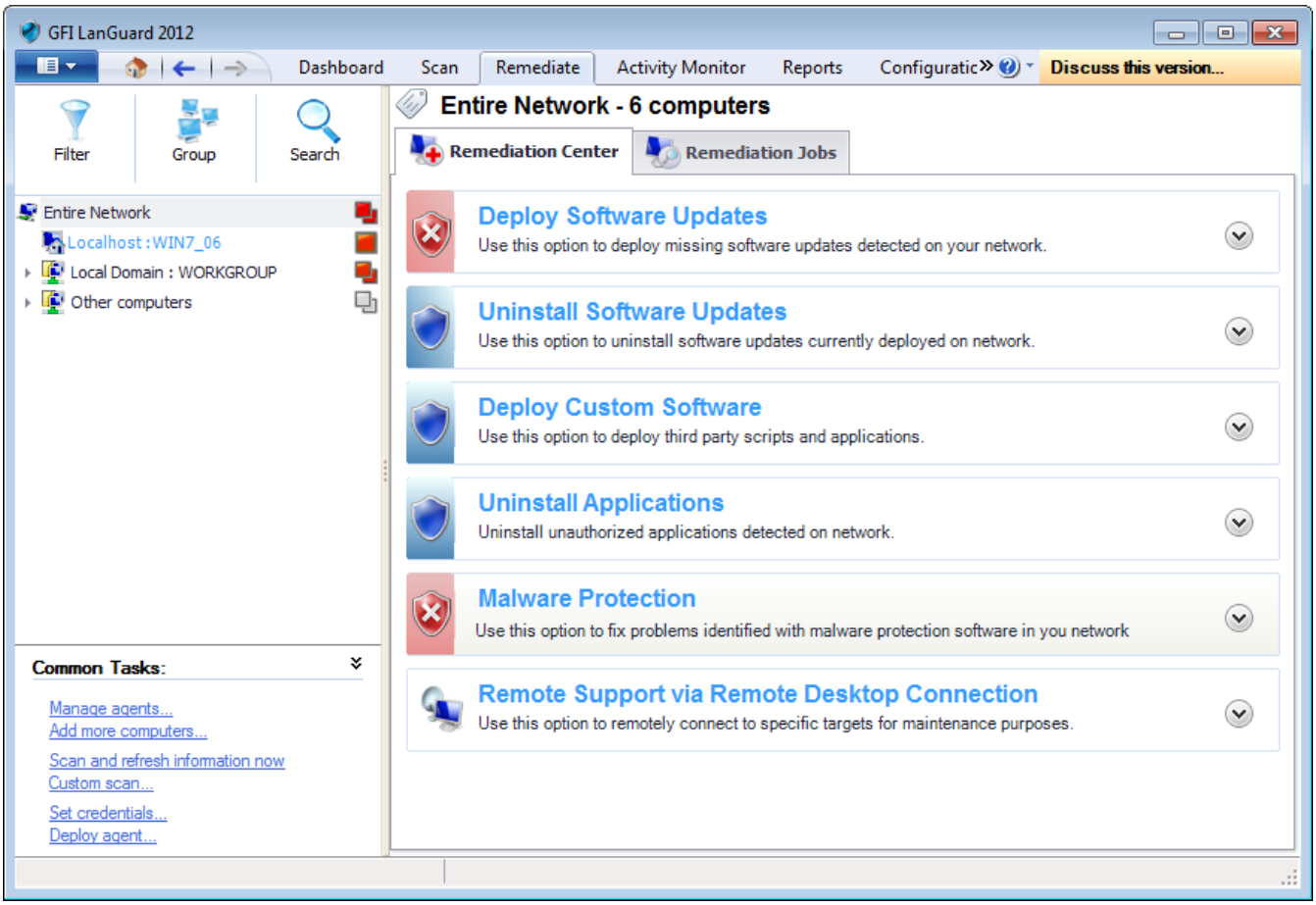
3. A complete list of Microsoft products for which GFI LanGuard can download and deploy patches is available at http://go.gfi.com/?pageid=ms_app_fullreport

4. Non-Microsoft software update patches supported by GFI LanGuard is available at http://go.gfi.com/?pageid=3p_fullreport

5. GFI LanGuard can be set to automatically download missing patches and service packs discovered during a network security scan. For more information, refer to Configuring missing updates auto-deployment (page 117).

8.2.2 Using the Remediation Center

The **Remediation Center** enables you to fix security issues found during a network scan by deploying or uninstalling applications from target machines. To access the **Remediation Center**, select **Remediate** tab > **Remediation Center**.



Screenshot 91: Remediation center

From the left panel, expand and locate a computer or a domain to perform remediation actions. The available remediation actions are described below:

Table 55: Remediation actions

Action	Description
Deploy Software Updates	Deploy missing patches discovered when auditing target computers. For more information, refer to Deploying Software Updates (page 139).
Uninstall Software Updates	Uninstall service packs from target computers. For more information, refer to Uninstalling Software Updates (page 142).
Deploy Custom Software	Deploy custom applications and scripts on target computers. For more information, refer to Deploying Custom Software (page 144).
Uninstall Applications	Uninstall applications from target computers. For more information, refer to Uninstalling Custom Applications (page 145).
Malware Protection	Perform Malware protection actions on target computers. For more information, refer to Malware Protection (page 147).
Remote Support via Remote Desktop Connection	Connect to a target machine and perform administrative tasks using remote desktop connection. For more information, refer to Using Remote Desktop Support (page 149).

8.2.3 Deploying Software Updates

Use the **Deploy Software Updates** feature to manually deploy:

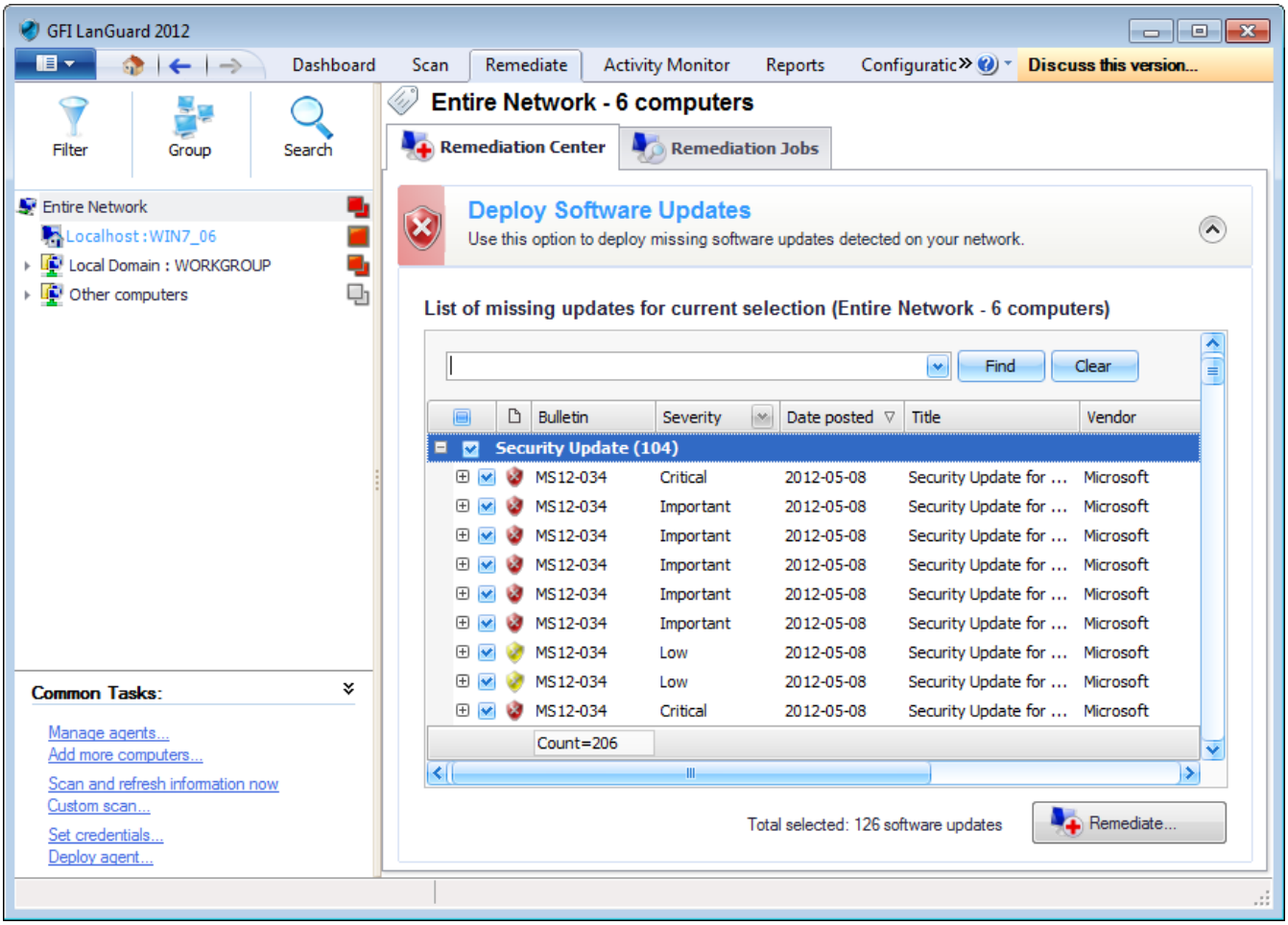
- Missing Service Packs and Update Rollups
- Missing Security Updates
- Missing Non-Security Updates.

This feature enables you to specifically select the items you want to deploy and provides you with a detailed description for each.

> **Note**
>
> To view additional information about an update, right-click on an update and select **More details > Bulletin info...**

To manually deploy software updates:

1. Launch GFI LanGuard.
2. Click **Remediate** tab and expand **Deploy Software Updates**.

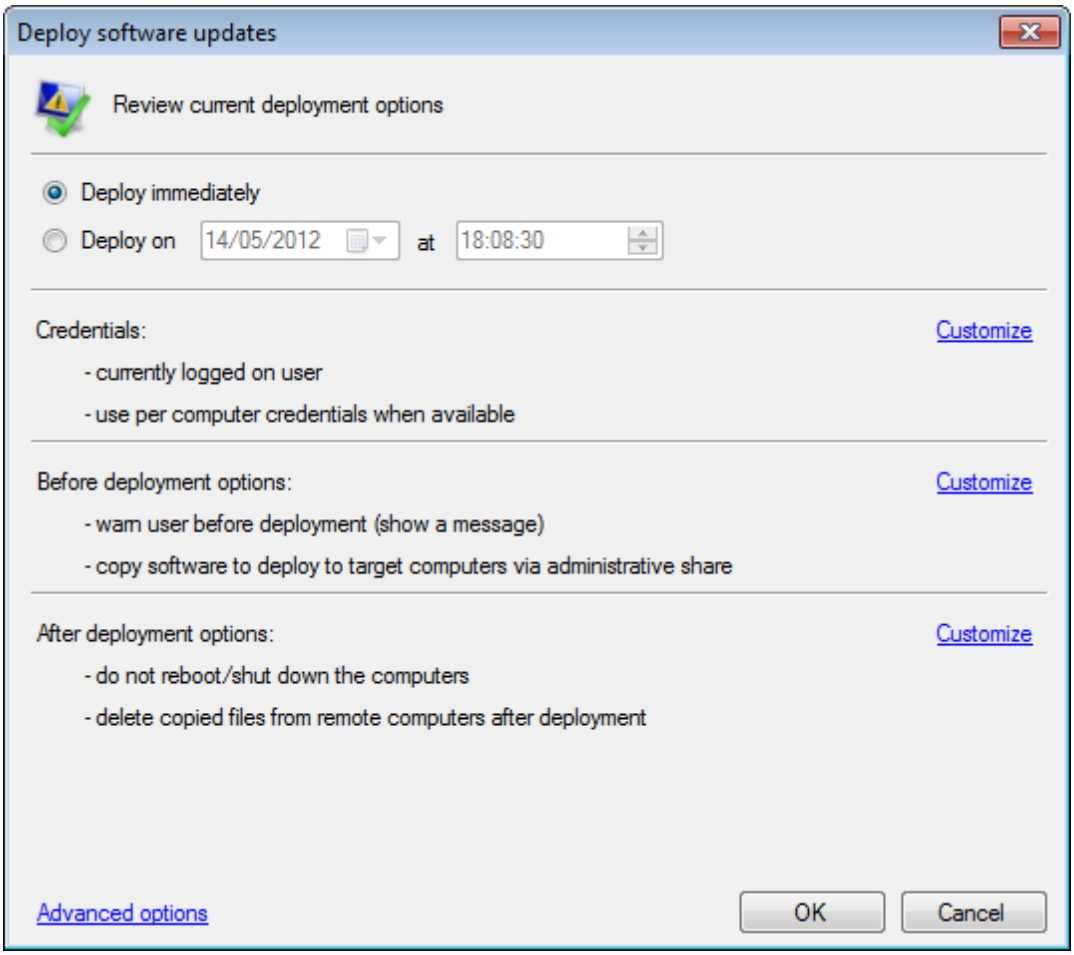


Screenshot 92: Deploying software updates

3. From the computer tree, select the computer/group where to deploy software updates.
4. From the **List of missing updates**, select the updates to deploy.

> **Note**
>
> Use the search bar to look for specific missing updates or use the filtering options for each column heading to view the required data only.

5. Click **Remediate**.



Screenshot 93: Deploy software updates options

6. The **Deploy software updates** dialog, enables you to edit deployment options before starting the deployment operation. Review the options described below:

Table 56: Deploy software updates options

Option	Description
Deploy immediately	Selected by default. Leave selected to deploy missing updates immediately.
Deploy on	Specify a date and time when to deploy missing updates .
Credentials	Provides you with the credentials settings for updates. Click **Customize** to change settings .
Before deployment options	Provides you with the actions taken before deploying software updates. Click **Customize** to edit the before deployment message, and the type of share created to transfer updates and scan details files.
After deployment options	Provides you with the actions taken after deploying missing software updates. Click **Customize** to configure whether the computer(s) reboot, shutdown or display a message to the end-user.
Advanced options	Click **Advanced options** to configure the: » Number of deployment threads. Maximum = 10 » Deployment timeout » Alternate credentials. Select **Remember settings** to reuse the same configuration when running the next deployment job. For more information, refer to Configuring auto-remediation options (page 125).

7. Click **OK** to start deploying updates. You are automatically taken to the **Remediation Jobs** tab where you can monitor the progress of the deployment operation.

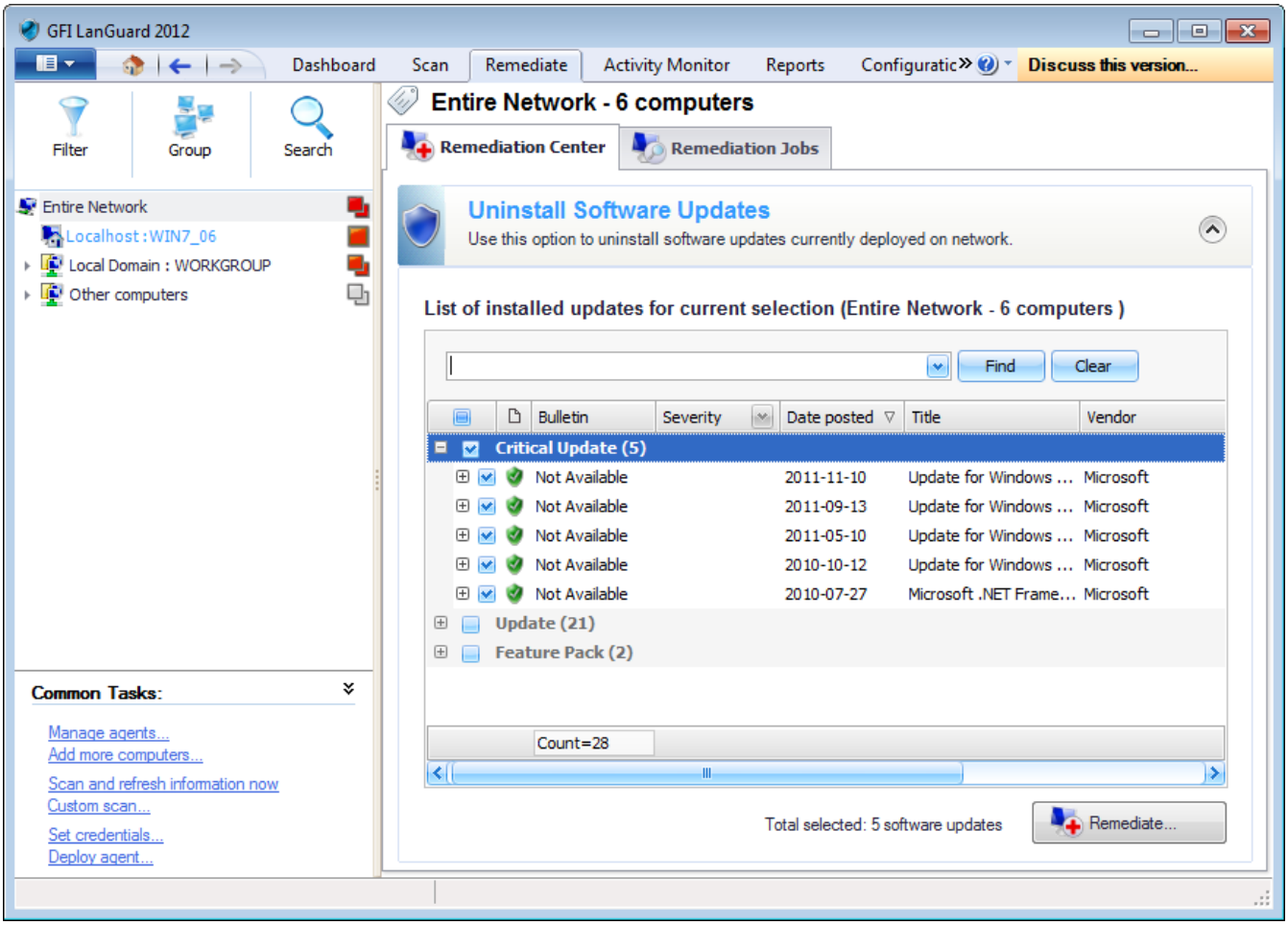
8.2.4 Uninstalling Software Updates

The **Uninstall Software Updates** feature enables you to manually remove:

- Installed Service Packs and Update Rollups
- Installed Security Updates
- Installed Non-Security Updates.

To manually uninstall software updates:

1. Launch GFI LanGuard.
2. Click **Remediate** tab and expand **Uninstall Software Updates**.

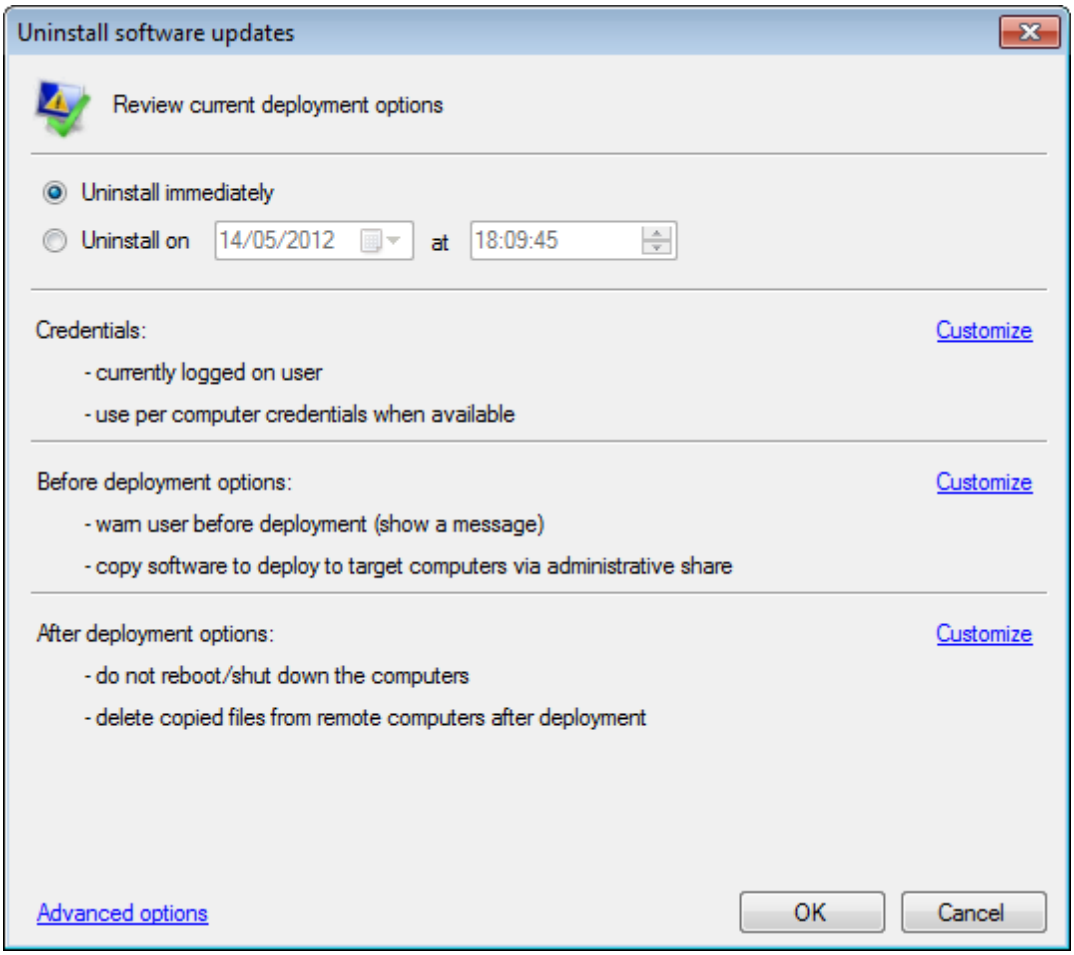


Screenshot 94: Uninstalling software updates

3. From the computer tree, select the computer/group where to uninstall software updates.
4. From the **List of installed updates**, select the updates you want to uninstall.

> **Note**
>
> Use the search bar to look for specific installed updates or use the filtering options for each column heading to view the required data only.

5. Click **Remediate**.



Screenshot 95: Uninstall software updates options

6. The **Uninstall software updates** dialog, enables you to edit uninstall options before starting the uninstall operation. Review the options described below:

Table 57: Uninstall software updates options

Option	Description
Uninstall immediately	Selected by default. Leave selected if you want to uninstall updates immediately.
uninstall on	Specify a date and time for when updates are uninstalled.
Credentials	Provides you with the credentials settings that are used to uninstall updates. Click **Customize** to change settings and use alternate credentials.
Before deployment options	Provides you with the actions taken before uninstalling software updates. Click **Customize** to edit the before deployment message, and shares mode used to transfer updates.
After deployment options	Provides you with the actions taken after uninstalling software updates. Click **Customize** to configure whether the computer(s) reboot, shutdown or display a message to the end-user.
Advanced options	Click **Advanced options** to configure the: » Number of deployment threads. Maximum = 10 » Deployment timeout » Alternate credentials. Select **Remember settings** to reuse them when running the next deployment operation. For more information, refer to Configuring auto-remediation options (page 125).

7. Click **OK** to start uninstalling the selected updates. You are automatically taken to the **Remediation Jobs** tab where you can monitor the progress of the uninstall operation.

8.2.5 Deploying Custom Software

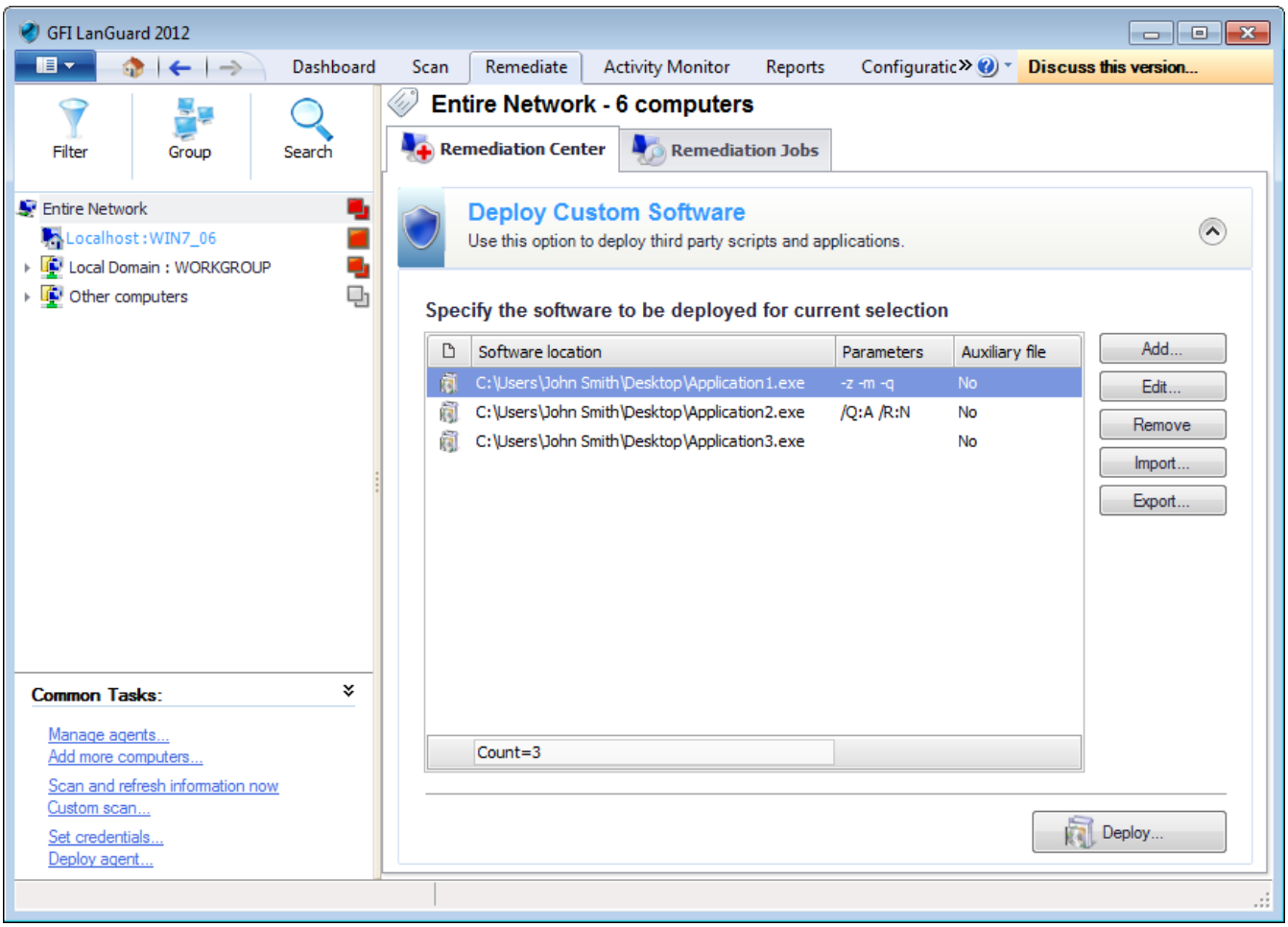
Apart from security updates and patches, GFI LanGuard also enables you to remotely deploy third party or custom software network-wide. Software that can be remotely deployed includes:

- Security applications such as anti-virus/anti-spyware solutions and software firewalls
- Third party software updates and patches such as anti-virus/anti-spyware signature file updates
- Custom code such as scripts and batch-files
- Desktop applications such as Microsoft® Office 2007 and more.

To specify which software to deploy:

1. Click on **Remediate** tab > **Remediation Center**.

2. From the computer tree, select the computers where the new software will be deployed and click **Deploy Custom Software**.



Screenshot 96: List of software to be deployed

3. Use the options described in below to add the applications to deploy:

Table 58: Options available in Deploy Custom Software

Option	Description
Add	Click this button to launch the Add custom software dialog. This dialog enables you to add an application to the list and if required configure parameters.
Edit	Select an application and click this button to launch the Add custom software dialog. This dialog enables you to modify the existing installation parameters.

Option	Description
Remove	Select an application from the list and click this button to remove the application.
Import	Click this button to import the applications parameters from an XML file.
Export	Click this button to export the applications parameters to XML file.

4. Click **Deploy** and configure the options described below:

Table 59: Deployment options

Option	Description
Deploy immediately	Deploy the selected applications immediately.
Deploy on	Deploy the selected applications on a specific date and time. Configure when to deploy the applications.
Credentials	Select the authentication method to use or specify a username and password. Select **Use per computer credentials when available**, to use the credentials specified in the computer properties. For more information, refer to Agent properties (page 47).
Before deployment options	Configure the actions to perform before deploying the selected applications. For more information, refer to Configuring auto-remediation options (page 125).
After deployment options	Configure the actions to perform after deploying the selected applications. For more information, refer to Configuring auto-remediation options (page 125).
Advanced options	Configure other options related to reboot/shut down and delete copied files from remote computers. For more information, refer to Configuring auto-remediation options (page 125).

5. Click **OK**.

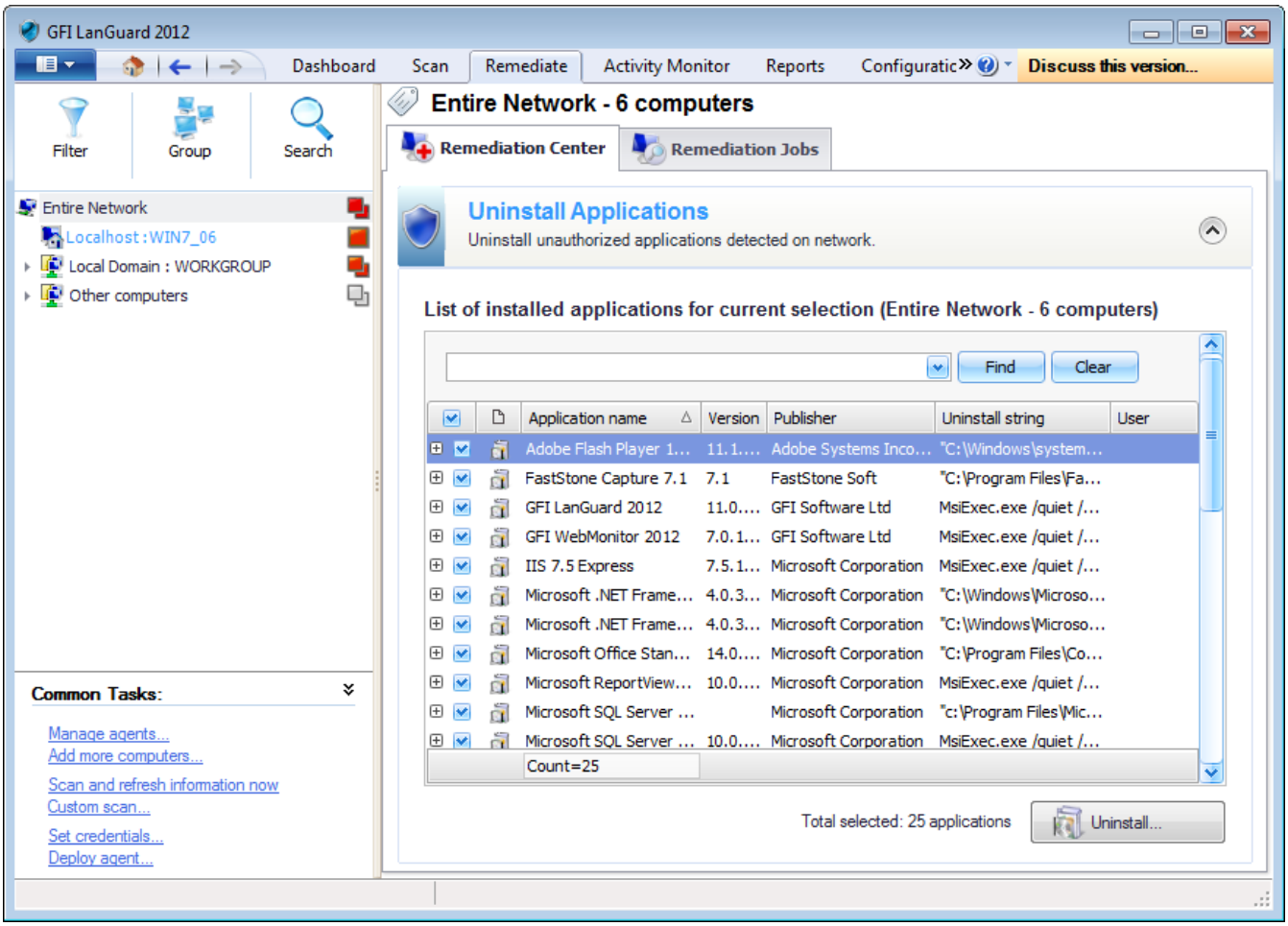
6. To view the deployment progress, click **Remediation Jobs** from the right panel.

8.2.6 Uninstalling Custom Applications

Using this feature, you can control the installed applications, on which computers, and uninstall any unauthorized applications present on network computers.

To uninstall applications:

1. Select **Remediate** tab > **Remediation Center** and click **Uninstall Applications**.



Screenshot 97: Uninstall applications

2. Expand the application to display the list of computers and select the computers where the application will be uninstalled.

> **Note**
>
> The list of applications displayed relies on the unauthorized applications set up for the scanning profile in use. For more information, refer to Configuring unauthorized applications auto-uninstall (page 121).

3. Repeat step 2 for all applications that will be uninstalled and click **Uninstall**.

> **Note**
>
> Key in a criteria and click **Find** to search a vulnerability. Click **Clear** to clear previous search results.

4. Configure the options described below:

Table 60: Uninstall applications

Option	Description
Uninstall immediately	Uninstall the selected applications immediately.

Option	Description
Uninstall on	Uninstall the selected applications on a specific date and time. Configure when to uninstall the applications.
Credentials	Select the authentication method to use or specify a username and password. Select **Use per computer credentials when available**, to use the credentials specified in the computer properties. For more information, refer to Agent properties (page 47).
Before deployment options	Configure the actions to perform before deploying the selected applications. For more information, refer to Configuring auto-remediation options (page 125).
After deployment options	Configure the actions to perform after deploying the selected applications. For more information, refer to Configuring auto-remediation options (page 125).
Advanced options	Configure other options related to reboot/shut down and delete copied files from remote computers. For more information, refer to Configuring auto-remediation options (page 125).

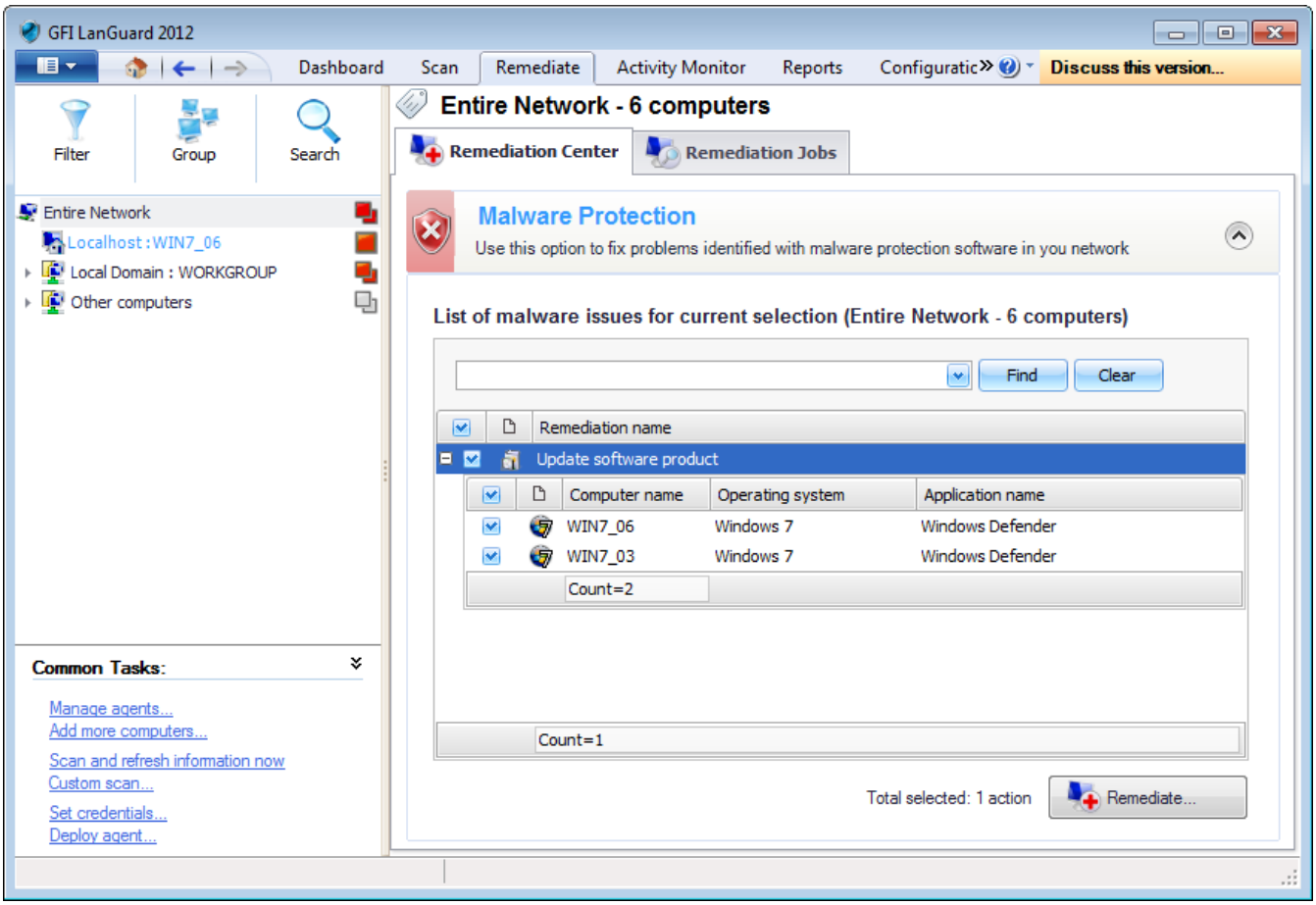
5. Click **OK**.

6. To view the un-installation progress, click **Remediation Jobs** from the right panel.

8.2.7 Malware Protection

Use the **Malware Protection** section to remediate vulnerabilities related to malware protection identified on target computers. Amongst others, this section enables you to scan target machines for spyware, viruses and enable local firewall.

> **Note**
>
> To scan a machine for viruses and spyware, the target machine must have anti-virus and anti-spyware installed.



Screenshot 98: Malware protection

To remediate malware protection vulnerabilities:

1. Select **Remediate** tab > **Remediation Center** and click **Malware Protection**.

2. Locate and expand the malware vulnerability and select the computers to remediate.

> **Note**
>
> Key in a criteria and click **Find** to search a vulnerability. Click **Clear** to clear previous search results.

3. Click Remediate and configure the options described below:

Table 61: Deployment options

Option	Description
Deploy immediately	Deploy the selected applications immediately.
Deploy on	Deploy the selected applications on a specific date and time. Configure when to deploy the applications.
Credentials	Select the authentication method to use or specify a username and password. Select **Use per computer credentials when available**, to use the credentials specified in the computer properties. For more information, refer to Agent properties (page 47).
Before deployment options	Configure the actions to perform before deploying the selected applications. For more information, refer to Configuring auto-remediation options (page 125).

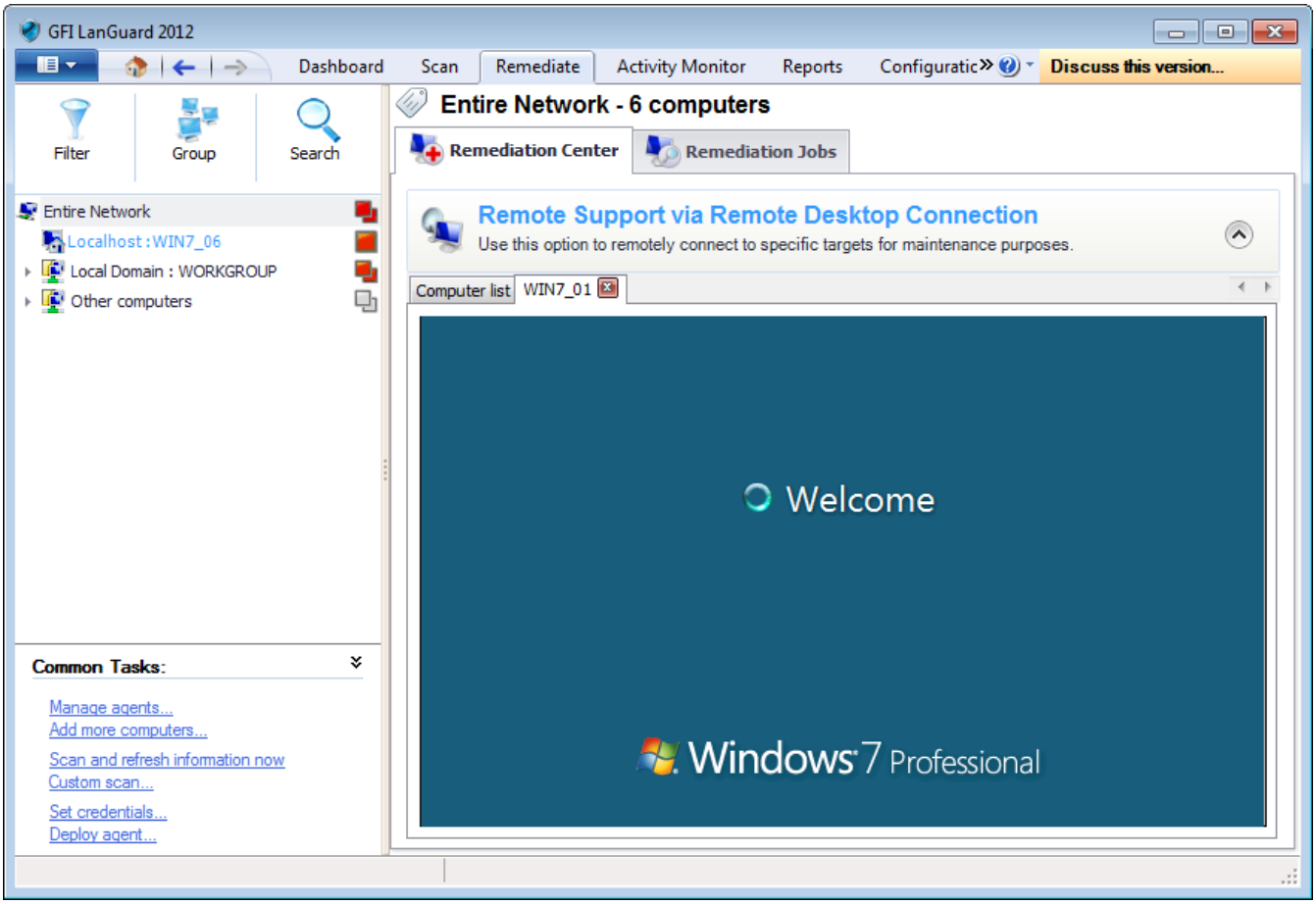
Option	Description
After deployment options	Configure the actions to perform after deploying the selected applications. For more information, refer to Configuring auto-remediation options (page 125).
Advanced options	Configure other options related to reboot/shut down and delete copied files from remote computers. For more information, refer to Configuring auto-remediation options (page 125).

4. Click **OK**.

5. To view the action progress, click **Remediation Jobs** from the right panel.

8.2.8 Using Remote Desktop Support

Through Remote Support, you can control remote computers using Terminal Services and Remote Desktop Protocol. Remote Support enables you to install missing patches, service packs and custom software through a remote connection.



Screenshot 99: Remote desktop connection

To connect remotely to a target machine:

1. Click **Remediate** tab and from the left panel select a computer or domain/workgroup.

2. Expand **Remote Support via Remote Desktop Connection** from the right panel.

3. Depending on your selection, the list contains the available computers that allow remote desktop connection.

4. Double-click a machine from the list to connect.

Note

To disconnect a machine, select **Remediation Center >Remote Support via…**, right-click a machine from the list and select **Disconnect**.

Note

To disable remote connection, right click a machine and select **Disable Remote Connection**.

9 Activity Monitoring

Monitoring enables you to learn more about how GFI LanGuard is performing in your infrastructure. The **Activity Monitor** tab in GFI LanGuard enables you to monitor active security scans, remediation jobs and download operations of missing updates and security definitions.

Topics in this chapter:

9.1 Monitoring Security Scans 151

9.2 Monitoring Software Updates Download 153

9.3 Monitoring Remediation Operations 155

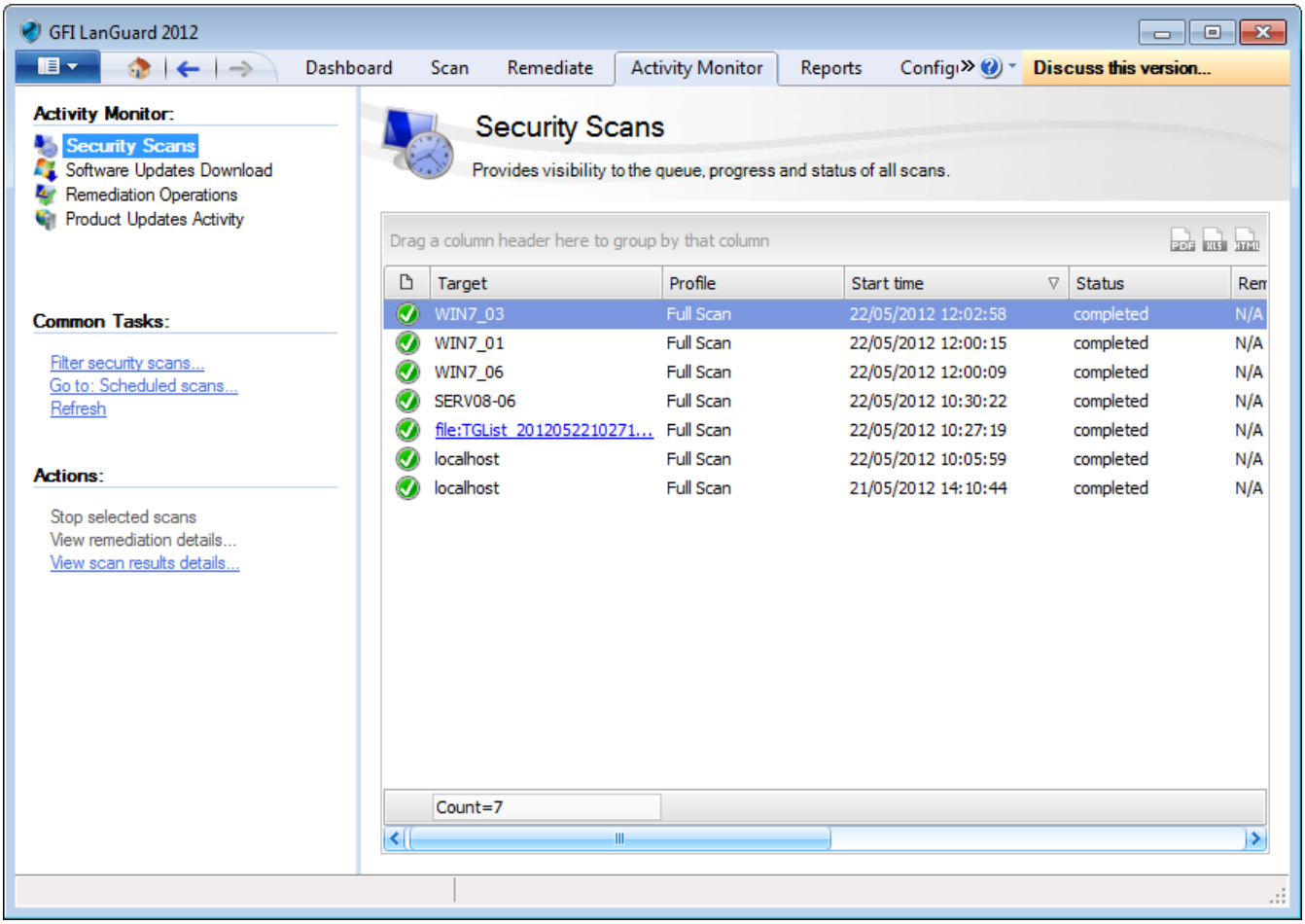
9.4 Monitoring Product Updates 158

9.1 Monitoring Security Scans

The **Security Scans** section enables monitoring of all the security scans that are currently in progress.

To monitor active security scans:

1. Launch GFI LanGuard.
2. Click **Activity Monitor** tab and from the left panel click **Security Scans**.



Screenshot 100: Monitoring security scans

Note

To stop a scan right-click the security scan and select **Stop selected scans**.

Note

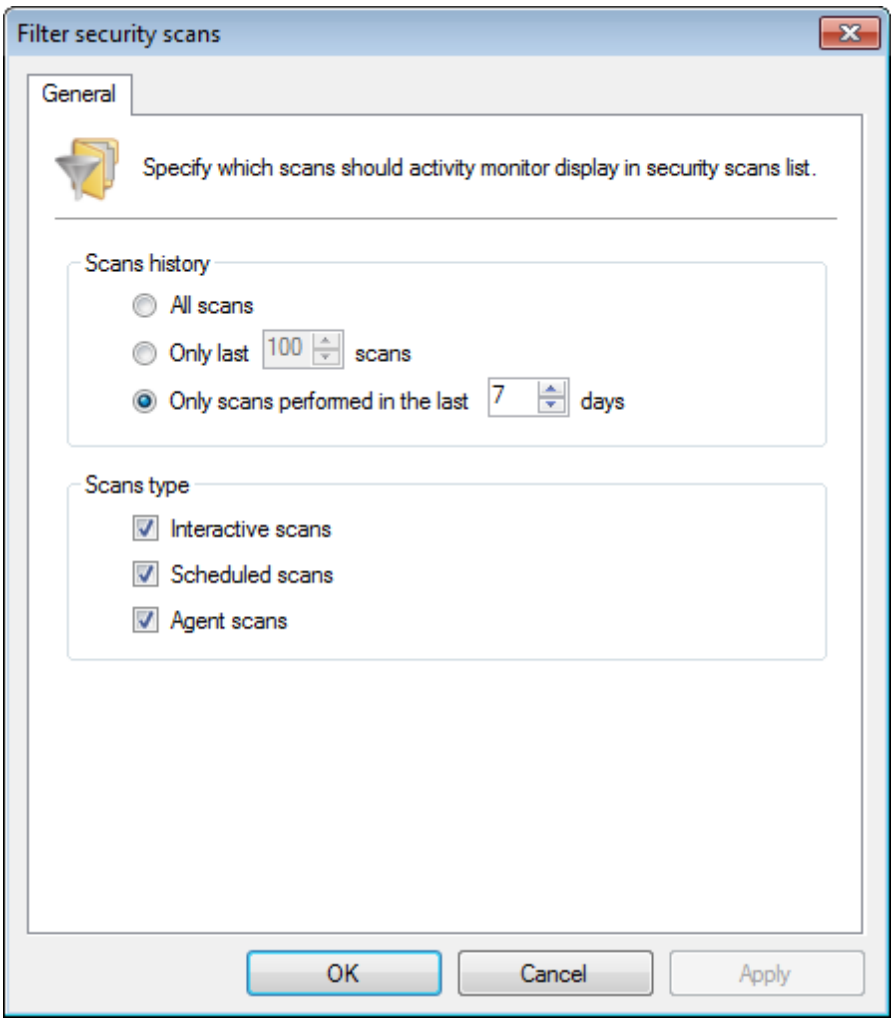
Drag and drop a column header in the designated area to group data by criteria.

9.1.1 Filter Security Scans

The **Security Scan** section enables you to configure what type of scans to monitor. To configure what type of scans are displayed:

1. Launch GFI LanGuard.

2. Click **Activity Monitor** tab and from **Common Tasks**, click **Filter security scans**.



Screenshot 101: Filter security scan dialog

3. Configure the options described below:

Table 62: Filter security scan dialog

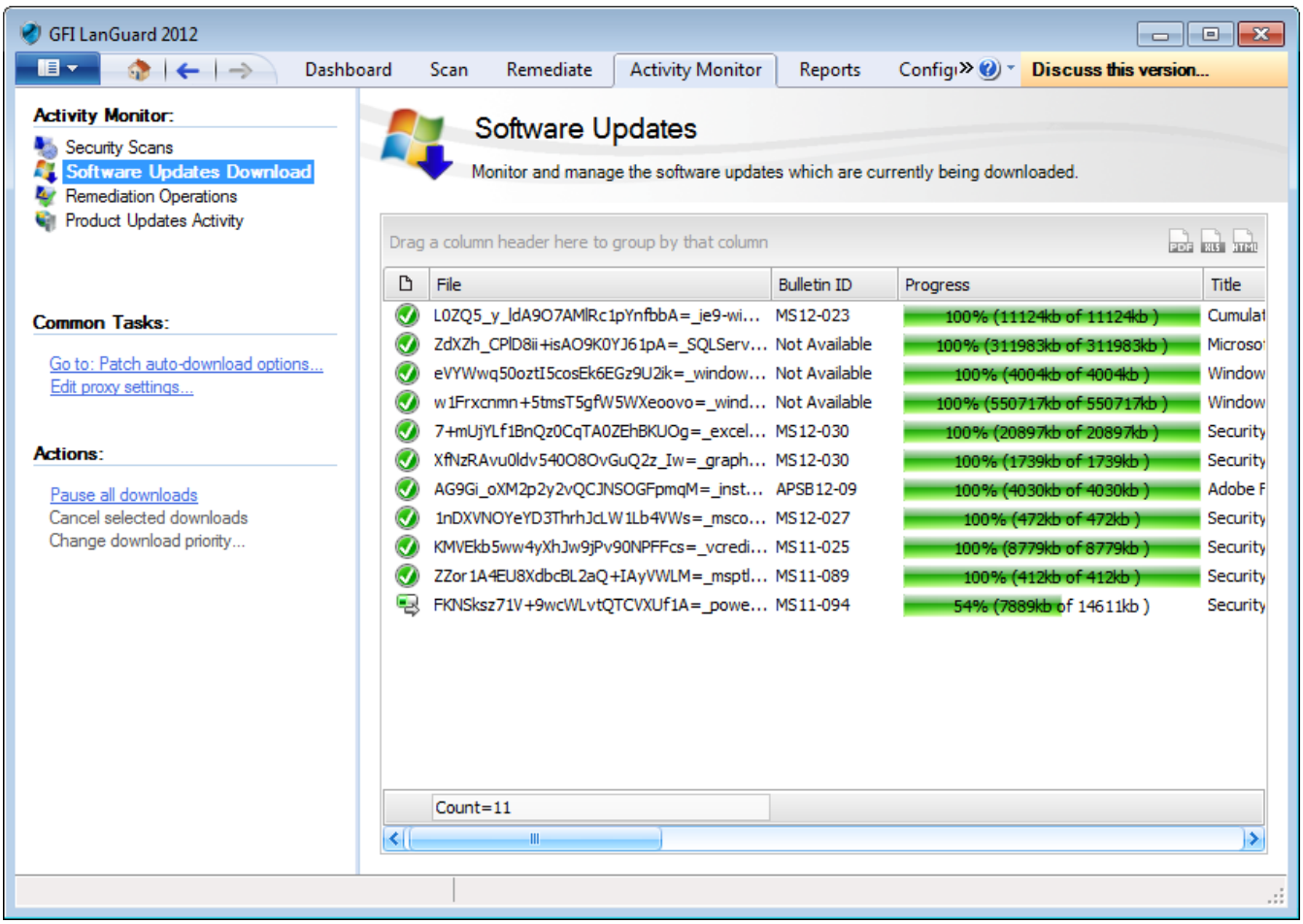
Option	Description
All scans	Displays all scans.

Option	Description
Only last X scans	Displays only the last X scans.
Only scans performed in the last X days	Displays only the scans performed in the last X days.
Interactive scans	Displays only manual scans. For more information, refer to Manual scans (page 66).
Scheduled scans	Displays only scheduled scans. For more information, refer to Scheduled scans (page 70).
Agent scans	Displays only scans performed on agent computers. For more information, refer to Starting an Agent scan manually (page 82).

4. Click **OK**.

9.2 Monitoring Software Updates Download

The **Software Updates Download** screen enables you to monitor, pause, cancel or change priority to all the scheduled patch downloads.


GFI LanGuard 2012
Dashboard
Scan
Remediate
Activity Monitor
Reports
Config
Discuss this version...
Activity Monitor:
Security Scans
Software Updates Download
Remediation Operations
Product Updates Activity
Common Tasks:
Go to: Patch auto-download options...
Edit proxy settings...
Actions:
Pause all downloads
Cancel selected downloads
Change download priority...
Software Updates
Monitor and manage the software updates which are currently being downloaded.
Drag a column header here to group by that column
File
Bulletin ID
Progress
Title
L0ZQ5_y_ldA9O7AMlRc1pYnfbbA=_je9-wi... MS12-023 100% (11124kb of 11124kb) Cumulat
ZdXZh_CPlD8ii+isAO9K0YJ61pA=_SQLServ... Not Available 100% (311983kb of 311983kb) Microso
eVYWwq50oztI5cosEk6EGz9U2ik=_window... Not Available 100% (4004kb of 4004kb) Window
w1Frxcnmn+5tmsT5gfW5WXeoovo=_wind... Not Available 100% (550717kb of 550717kb) Window
7+mUjYLf1BnQz0CqTA0ZEhBKUOg=_excel... MS12-030 100% (20897kb of 20897kb) Security
XfNzRAvu0ldv540O8OvGuQ2z_Iw=_graph... MS12-030 100% (1739kb of 1739kb) Security
AG9Gi_oXM2p2y2vQCJNSOGFpmqM=_inst... APSB12-09 100% (4030kb of 4030kb) Adobe F
1nDXVNOYeYD3ThrhJcLW1Lb4VWs=_msco... MS12-027 100% (472kb of 472kb) Security
KMVEkb5ww4yXhJw9jPv90NPFFcs=_vcredi... MS11-025 100% (8779kb of 8779kb) Security
ZZor1A4EU8XdbcBL2aQ+IAyVWLM=_msptl... MS11-089 100% (412kb of 412kb) Security
FKNSksz71V+9wcWLvtQTCVXUf1A=_powe... MS11-094 54% (7889kb of 14611kb) Security
Count=11

Screenshot 102: Security updates download

The icon in the first column indicates the download status. The table below describes the different states:

Table 63: Updates download status

Icon	Description
	Downloaded Update downloaded successfully.
	Downloading Update is being downloaded.

Icon	Description
	Failed An error occurred while downloading the update. Refer to Error column for more details regarding the error encountered.
	Pending Update is queued for download.
	Cancelled User cancelled update download.

Right-click an entry and select one of the options described below:

Table 64: Security updates download

Option	Description
Configure Patch Auto-Download	Enables or disables auto-patch download and used to configure where the patches are stored. For more information, refer to Patch auto-download settings.
Edit proxy settings...	Configure the proxy settings used by GFI LanGuard to connect to the Internet. For more information, refer to Configuring Program Updates (page 184).
Change download priority...	Change the download priority. Select between, High, normal or low priority.
Cancel selected downloads	Stop and remove the selected download.
Pause all downloads	Temporarily pause all downloads.

9.2.1 Troubleshooting failed Software Updates

This section provides you with information about three software update errors, which are likely to cause software updates to fail from downloading and/or installing.

The table below provides you with the actual error message that you will receive if one of the errors has to occur and a possible cause and solution, for each:

Table 65: Troubleshooting failed Software Updates

Error Message	Cause	Solution
The file URL points to a different file than expected. Try re-scanning with the latest program updates	The Third-Party vendor replaces old patches with updated patches, using the same URL. GFI has no control over how Third-Party vendors replace updates and URLs.	Download the latest Product Updates manually and re-scan your targets. For more information, refer to Configuring Program Updates (page 184). **Note** There is a 12 to 24 hour delay between Third-Parties releasing new updates and GFI LanGuard adding support for them. During this time, you will continue to receive the error message, even though you download and scan your targets using the latest product updates.

Error Message	Cause	Solution
The repository folder is not accessible. See Configuration - Patch Auto-download	The repository folder is the location where updates are downloaded to. GFI LanGuard enables you to specify alternate repositories than the default location. This error is generally caused after specifying an invalid or inaccessible repository path (example, the given path refers to a location on a shutdown computer).	1. Manually check that you can access the folder path, using the same logon credentials. 2. Ensure that the specified path is a valid: » **Local path** - example: `C:\Share` or `C:\Folder` » **UNC path** - example: `\\NetworkShare\Folder` 3. Ensure that the path is keyed in correctly. **Note** For more information, refer to **Configuring Patch Auto-download settings**, from Configure Missing Updates Auto-Deployment.
Internet connection not available	The computer where GFI LanGuard is installed, does not have Internet access. There are many possible causes to this problem.	Establish an Internet connection and attempt to download the failed updates.

9.3 Monitoring Remediation Operations

Remediation operations can be monitored from the following places:

» Remediation Jobs sub-tab

» Remediation Operations view

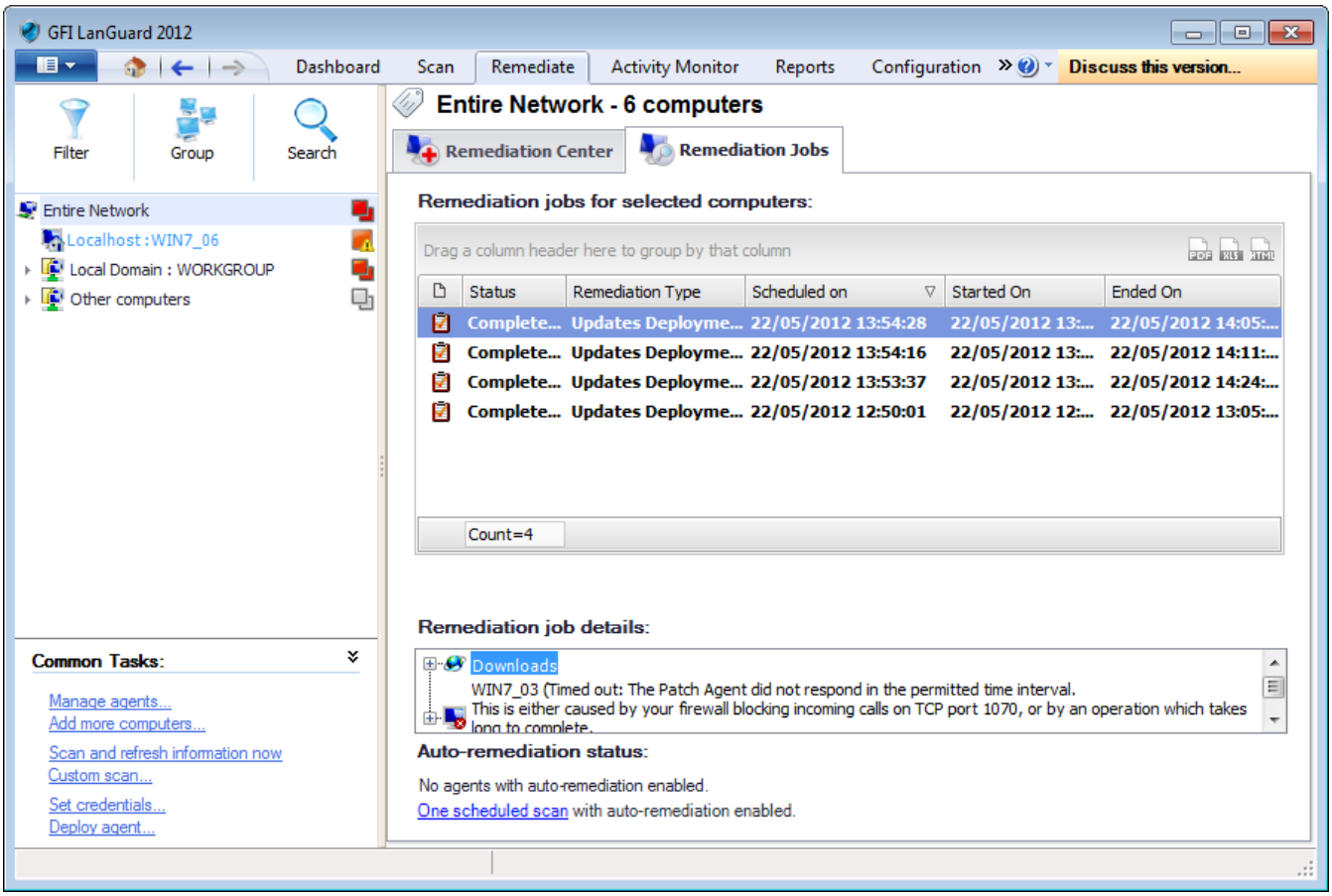
9.3.1 Remediation Jobs sub-tab

The **Remediation Jobs** section enables you to monitor the remediation actions currently in progress.

To view remediation jobs in progress:

1. Launch GFI LanGuard.

2. Click **Remediate** tab > **Remediation Jobs** sub-tab.



Screenshot 103: Monitoring jobs from the Remediation jobs sub-tab

3. From the computer tree, select **Entire Network** to view all the running, as well as completed operations. Select specific computers/groups to view remediation jobs history and/or remediation progress for the selected item(s).

Note

Right-click a remediation job and select **Cancel selected deployment** to stop the operation.

Note

Right-click a remediation job and select **Go to associated schedule scan** to view the pre-configured scan which triggered the remediation.

Note

The **Remediation job details** section provides you with granular progress details indicating the total number of files that have to be downloaded, download progress for each file and the current operation being executed as part of the remediation job.

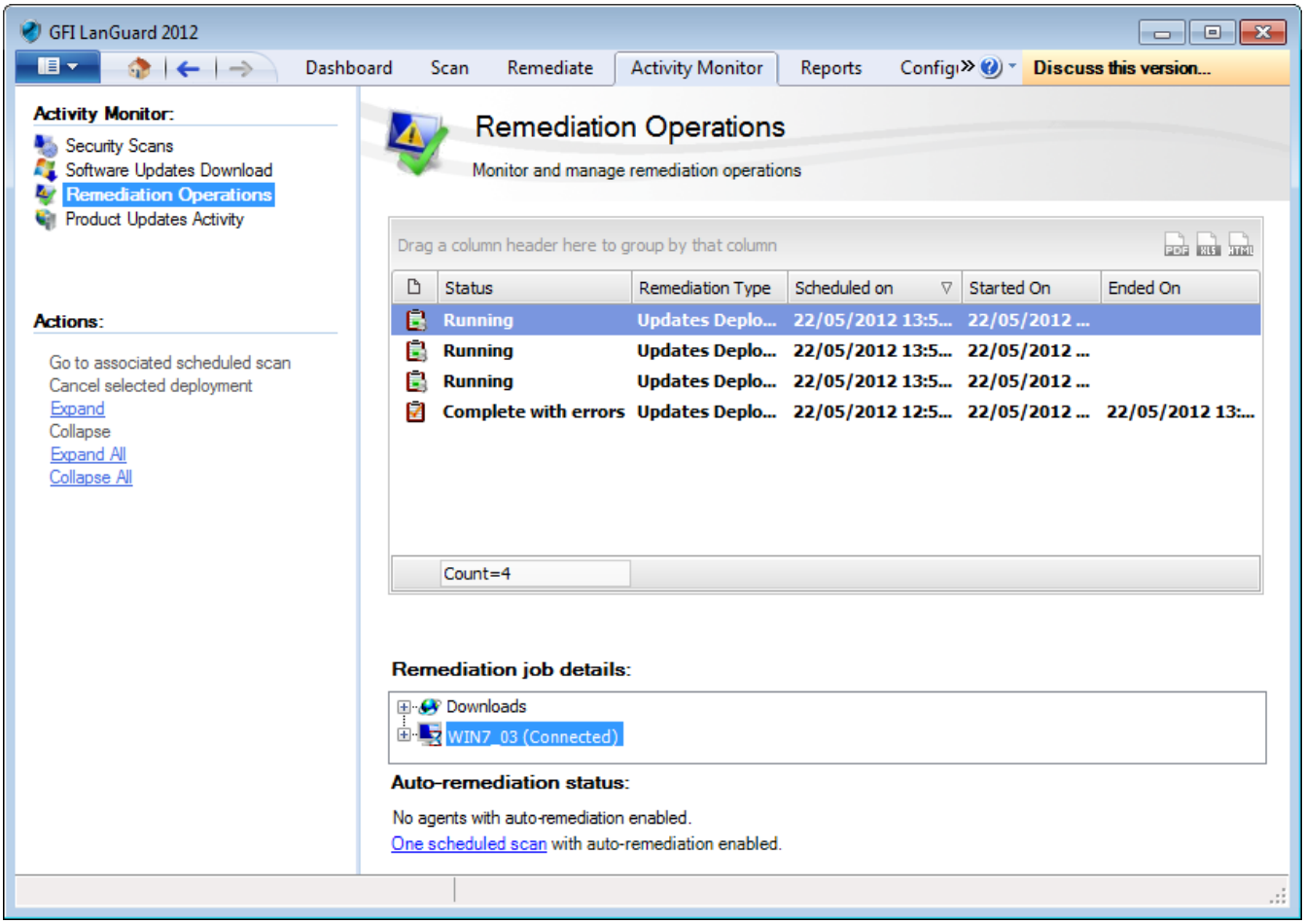
9.3.2 Remediation Operations view

The remediation operations screen enables you to monitor as well as cancel all the scheduled remediation features within GFI LanGuard.

To view remediation job activity:

1. Launch GFI LanGuard.

2. Click **Activity Monitor > Remediation Operations**.



Screenshot 104: Monitoring jobs from the Remediation Operations view

3. Use the view to monitor the status and history of all the running and complete remediation jobs.

Note

Right-click a remediation job and select **Cancel selected deployment** to stop the operation.

Note

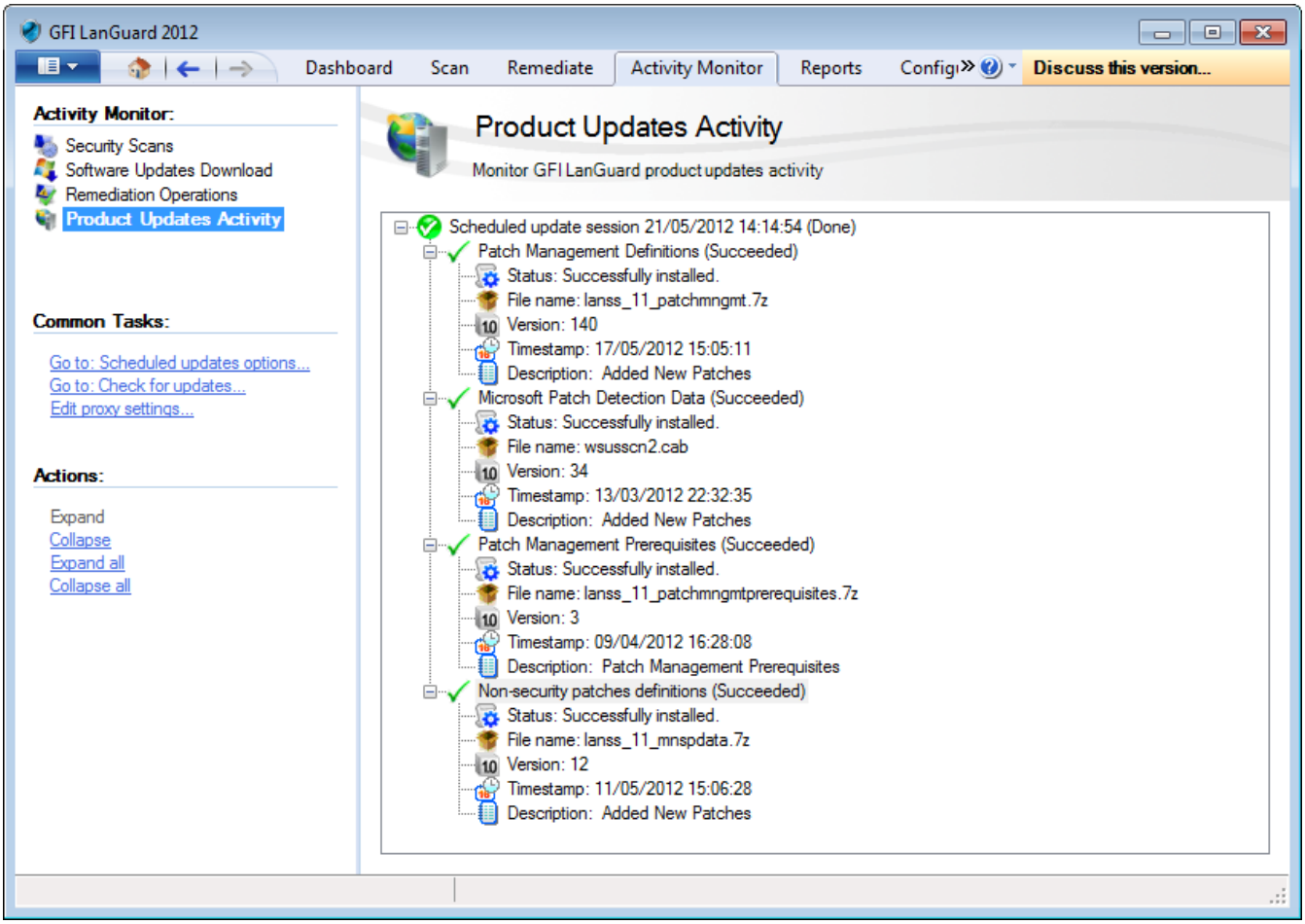
Right-click a remediation job and select **Go to associated schedule scan** to view the pre-configured scan which triggered the remediation.

Note

The **Remediation job details** section provides you with granular progress details indicating the total number of files that have to be downloaded, download progress for each file and the current operation being executed as part of the remediation job.

9.4 Monitoring Product Updates

The **Product Updates Activity** screen enables you to view a history of the product updates, performed by GFI LanGuard. For more information, refer to Configuring Program Updates (page 184).



Screenshot 105: Product updates activity

10 Reporting

GFI LanGuard includes a reporting module which enables you to generate text and graphical reports based on information obtained from network security scans. This chapter provides you with an overview of the available reports as well as how to create your own reports for a tailored solution. Through the Reports tab, you are able to generate technical activity reports for IT staff and also executive reports that normally contain less technical details and focus more on overall statistics.

Topics in this chapter:

10.1 Available reports 159

10.2 Generating reports 165

10.3 Scheduling Reports 167

10.4 Customizing default reports 170

10.5 Full text searching 174

10.1 Available reports

This section provides you with information about the reports that are available by default in the **Reports** tab of GFI LanGuard. There are two main types of reports:

- **General Reports** - provide detailed technical reports as well as executive summary reports about LAN security and patch management activity
- **Legal Compliance Reports** - provide system and network audit information that enable you to be compliant with standards, laws and regulations related to corporate network usage and management conventions.

Refer to the following sections for information about:

- Available general reports
- Available legal compliance reports

10.1.1 General reports

To view **General** reports:

1. Click **Reports** tab.

2. From the list of reports, expand **General** and select any of the following reports:

Table 66: Available General Reports

Report Title	Description
Network Security Overview	An executive summary report showing: » Network vulnerability level » Most vulnerable computers » Agent status » Audit status » Vulnerability trends over time » Information on operating systems » Servers and workstations.
Computer Security Overview	An executive summary report showing: » Computer vulnerability level » Agent status » Audit status » Vulnerability trends over time » Computer summary and details.
Vulnerability Status	Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by: » Computer name » Vulnerability severity » Timestamp » Category.
Patching Status	Shows statistical information related to missing and installed updates detected on your scan targets. Updates can be grouped by name, severity, timestamp, vendor and category. Use this report to get: » Missing vs. Installed updates comparison » Charts and tables displaying missing updates distribution for each item from the first and second grouping criteria » Charts and tables displaying installed updates distribution for each item from the first and second grouping criteria » Patching details for missing and installed patches.
Missing Microsoft® Security Updates	Shows statistical information related to missing Microsoft® security updates, detected on your scan targets. Select items to include in your report: » General missing updates distribution chart » Distribution table » Vulnerability list.
Missing Non-Microsoft® Security Updates	Shows statistical information related to missing non-Microsoft® security updates, detected on your scan targets. Select items to include in your report: » General missing updates distribution chart » Distribution table » Vulnerability list.
Missing Security Updates	Lists statistical information related to missing security updates, found on scanned computers.

Report Title	Description
Full Audit	A technical report showing information retrieved during an audit. Amongst others, the report contains information on: » Vulnerabilities » Open ports » Hardware and software.
Computer Summary	A summary of scan target information, including: » Operating system information » Agent status » Vulnerabilities severity.
Hardware Audit	Illustrates information related to the hardware found during an audit.
Computer Details	Provides a detailed list of computer properties, including: » MAC Address » Time to Live » Network Role » Domain » Lan Manager » Is relay agent » Uses relay agent » Attributes » Operating system » IP address.
Open Shares	Lists all the shared folders found during an audit. The results are grouped by computer name.
Open Ports	Lists all the open ports found during an audit. The result are grouped by port type (TCP and UDP).
Scan Based - Full Audit	A technical report showing information retrieved during a specified scan. The report contains full details of the scanned computers and also auto-remediation performed after that scan.
Last Scan Summary	A technical report containing the summary of the information retrieved during the last scan.
Last Scan Details	A technical report containing all the information during the last scan. The report contains full details for the scanned target.
Last Auto-remediation	A technical report containing all the information related to auto-remediation performed after the last scan.
Last Scan Security Changes	Shows all changes detected during the last scan.
Software Audit	Shows all unauthorized applications installed on target machines found during an audit. Amongst others, the report includes information on: » Antivirus » Anti-spyware » Applications inventory.
Unauthorized Applications	Lists all unauthorized applications installed scan targets.
Antivirus Applications	Shows information related to the antivirus installed on scan targets.

Report Title	Description
Scan History	An overview of the network security audits performed over time. Amongst others, the report includes information on: » Most scanned computers » Least scanned computers » Auditing status » History listing.
Remediation History	Shows information related to remediation actions performed on target computers. Amongst others, the report includes information on: » Remediation actions per day » Remediation distribution by category » Remediation list grouped by computers.
Network Security History	Shows the changes done on scan targets between audits. Amongst others, the report includes changes related to: » The vulnerability level » User accounts » Groups » Ports » Shares » Registry entries.
Baseline Comparison	Enables you to compare the results of all scan targets to a base computer. From the drop down list select the base computers and click Generate. The results are grouped by computer name and amongst others includes information on: » Registry » Installed Service Packs and Update Rollups » Missing Security/Non-Security Updates » Vulnerability level.

10.1.2 Legal Compliance reports

To view **Legal Compliance** reports:

1. Click **Reports** tab.

2. From the list of reports, expand any of the following compliance reports suites and select the report you want to generate:

Table 67: Available Legal Compliance Reports

Report Suite Title	Description
PCI DSS Compliance Reports	The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. GFI LanGuard provides you with a number of reports that cater for PCI DSS compliance, including: » PCI DSS Requirement 1.4 - Installed Firewall Applications » PCI DSS Requirement 2.2.3 - Disk Encryption Applications » PCI DSS Requirement 5.2 - Antivirus Applications » PCI DSS Requirement 6.1 - Remediation History by Date » PCI DSS Requirement 12.12 - Open Trojan Ports by Host.

Report Suite Title	Description
HIPAA Compliance Reports	The Health Insurance Portability and Accountability Act (HIPAA) is a requirement of all healthcare providers that regulates the exchange of private patient data. This helps prevent unlawful disclosure or release of medical information. To help you follow HIPAA regulations, GFI LanGuard provides you with a suite of HIPAA compliance reports, including: » HIPAA 164.308(a)(1)(ii)(A) - Missing Security Updates by Host » HIPAA 164.308(a)(1)(ii)(A) - Vulnerability Distribution by Host » HIPAA 164.308(a)(4)(ii)(A) - Open Ports » HIPAA 164.308(a)(5)(ii)(D) - Audit Policy » HIPAA 164.308(a)(8) - Baseline Changes Comparison.
SOX Compliance Reports	The Sarbanes-Oxley Act (SOX) is regulation created in response to high-profile financial scandals as well as to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. GFI LanGuard provides a list of SOX compliance reports, including: » SOX 302.a - Network Vulnerability Summary » SOX 302.a - Remediation History by Host » SOX 302.a - Security Scans History » SOX 404 - Vulnerability Listing by Category » SOX 404 - Missing Security Updates by Host.
GLBA Compliance Reports	The Gramm-Leach-Bliley Act (GLBA) is an act that allows consolidation between Banks and Insurance companies. Part of the act focuses on IT network compliance for such companies. GFI LanGuard offers a list of GLBA Compliance reports, including: » GLBA 501.b - Baseline Changes Comparison » GLBA 501.b - Network Patching Status » GLBA 501.b - Open Trojan Ports by Host » GLBA 501.b - Vulnerable Hosts Based on Open Ports » GLBA 501.b - Vulnerable Hosts by Vulnerability Level.
PSN CoCo Compliance Reports	The Public Service Network - Code of Connection (PSN CoCo) is simply a list of conditions that should be met before connecting an accredited network to another accredited network. GFI LanGuard helps you monitor the status of such connections through the list of PSN CoCo Compliance reports, which include: » PSNCoCo RIS. 1 - Baseline Changes Comparison » PSNCoCo MAL. 1 - Disk Encryption Applications » PSNCoCo MAL. 1 - Installed Firewall Applications » PSNCoCo PAT. 1 - Installed Security Updates by Host » PSNCoCo PAT. 1 - Installed Security Updates by Severity.
FERPA Compliance Reports	The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. GFI LanGuard provides a list of FERPA Compliance reports, including: » FERPA 20 USC 1232g (b) - Network Patching Status » FERPA 20 USC 1232g (b) - Network Security Log by Host » FERPA 20 USC 1232g (b) - Remediation History by Date » FERPA 20 USC 1232g (b) - Vulnerability Distribution by Host » FERPA 20 USC 1232g (b) - Vulnerable Hosts Based on Open Ports.

Report Suite Title	Description
ISO/IEC 27001 & 27002 Compliance Reports	The Information technology – Security techniques – Information security management systems (ISO/IEC) standard formally specifies a management system that is intended to bring information security under explicit management control. GFI LanGuard offers an extensive list of ISO/IEC Compliance reports, including: » ISO/IEC 27001 A. 10.4 - Antivirus Applications » ISO/IEC 27001 A. 10.7.2 - Disk Encryption Applications » ISO/IEC 27001 A. 10.6.2 - Open Shares » ISO/IEC 27001 A. 10.6.2 - Services » ISO/IEC 27001 A. 10.6.2 - System Information.
FISMA Compliance Reports	The Federal Information Security Management Act (FISMA) assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. GFI LanGuard helps you be compliant to FISMA standards through the provided reports, which include: » FISMA NIST SP 800-53 AC-2 - Groups and Users » FISMA NIST SP 800-53 PM-5 - Computer Details » FISMA NIST SP 800-53 PM-5 - Computer Summary » FISMA NIST SP 800-53 SI-5 - Missing Security Updates by Host » FISMA NIST SP 800-53 SI-7 - Antivirus Applications.
CAG Compliance Reports	The Consensus Audit Guidelines (CAG) is a publication of best practice guidelines for computer security. The project was initiated as a response to extreme data losses experienced by organizations in the US defense industrial base. GFI LanGuard offers a list of CAG Compliance reports, including: » CAG CC1 - Hardware Audit » CAG CC1 - Scan History » CAG CC3 - Audit Policy » CAG CC3 - Low Security Vulnerabilities » CAG CC11 - Open Ports.
NERC CIP Compliance Reports	The North American Electric Reliability Corporation (NERC) develops standards for power system operation, monitoring and enforcing compliance with those standards, assessing resource adequacy, and providing educational and training resources as part of an accreditation program to ensure power system operators remain qualified and proficient. GFI LanGuard provides a list of NERC CIP Compliance reports, including: » NERC CIP-005 R2 - Installed Firewall Applications » NERC CIP-005 R2 - Open Ports » NERC CIP-007 R2 - Open Shares » NERC CIP-007 R2 - Services » NERC CIP-007 R2 - System Information.

10.2 Generating reports

GFI LanGuard ships with an extensive list of default reports. These can be used as they are, or modified to provide information precisely to your requirements.

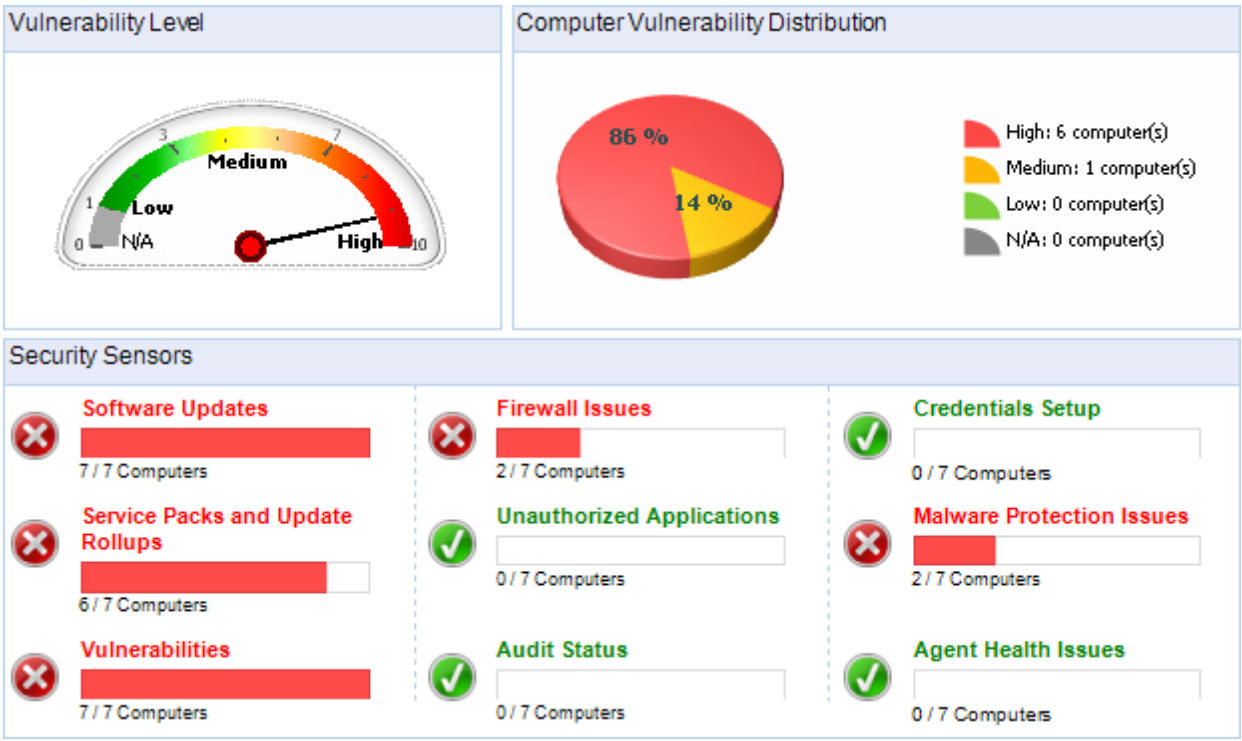
> **Note**
>
> For more information, refer to Customizing default reports (page 170).

To generate a report:

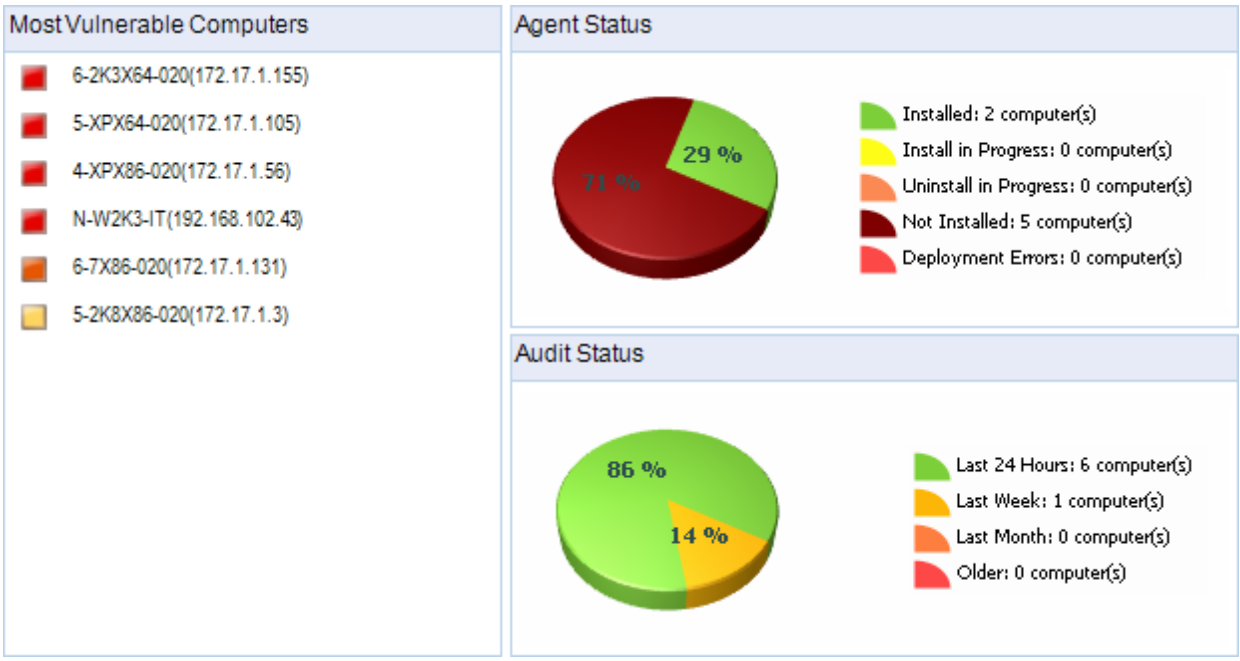
1. Click **Reports** tab.
2. From the computer tree, select the computer/group you want to report on.

> **Note**
>
> Select **Entire Network** to report on all the computers listed under the computer tree.

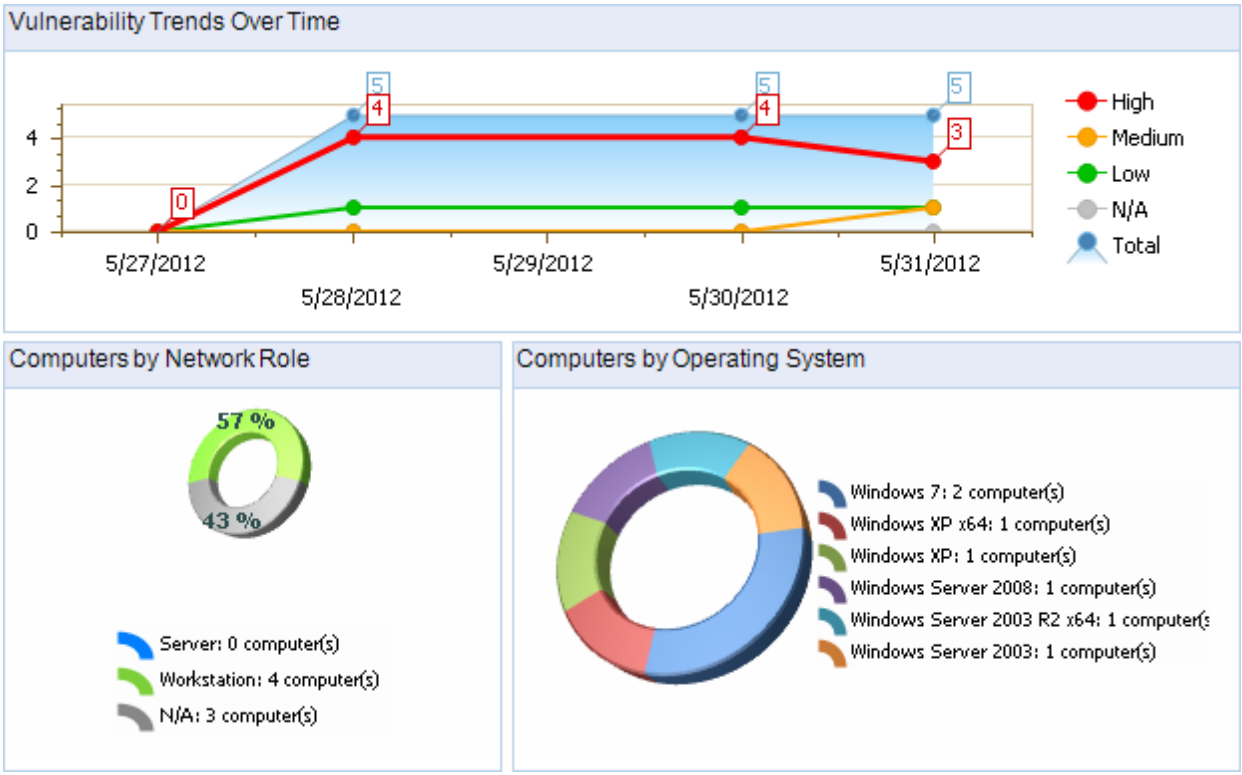
3. From the reports list, select the report you want to generate.
4. (Optional) From the right pane, click **Customize report** if changes to report items are required.
5. Click **Generate report**.



Screenshot 106: Report sample - Part 1



Screenshot 107: Report sample - Part 2



Screenshot 108: Report sample - Part 3

10.3 Scheduling Reports

To automate reporting tasks, GFI LanGuard enables you to generate and optionally send reports, based on a schedule. You can configure schedules for existing or custom reports.

This section contains information about:

- Creating new scheduled reports
- Configuring scheduled reports options
- Managing scheduled reports

10.3.1 Creating new scheduled reports

To create a new scheduled report:

1. Click **Reports** tab.

2. From **Actions**, select **New scheduled report**.

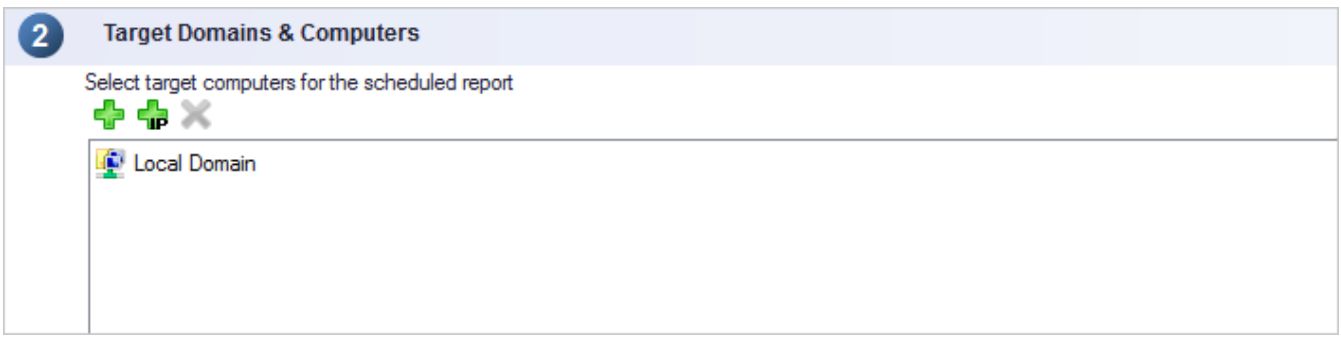
1
Report Template
Schedule Report Template:
Network Security Overview
Schedule Report Name:
Schedule for report 'Network Security Overview'
Schedule Report Description:
An executive summary report showing network vulnerability level, most vulnerable computers, agent status and audit status, vulnerability trends over time, information on operating systems, servers and

Screenshot 109: Select scheduled report template

3. From the **Report Template** section, configure the following options:

Table 68: Scheduled report template options

Option	Description
Schedule Report Template	Select an existing report from the drop-down menu. This enables you to create a new report based on the settings of an existing one.
Schedule Report Name	Key in a unique name for the new report.
Schedule Report Description	Optionally, key in some information about the report such as report items or schedule settings.



Screenshot 110: Add or remove target domains and/or computers

4. From the **Target Domains & Computers** section, configure the following options:

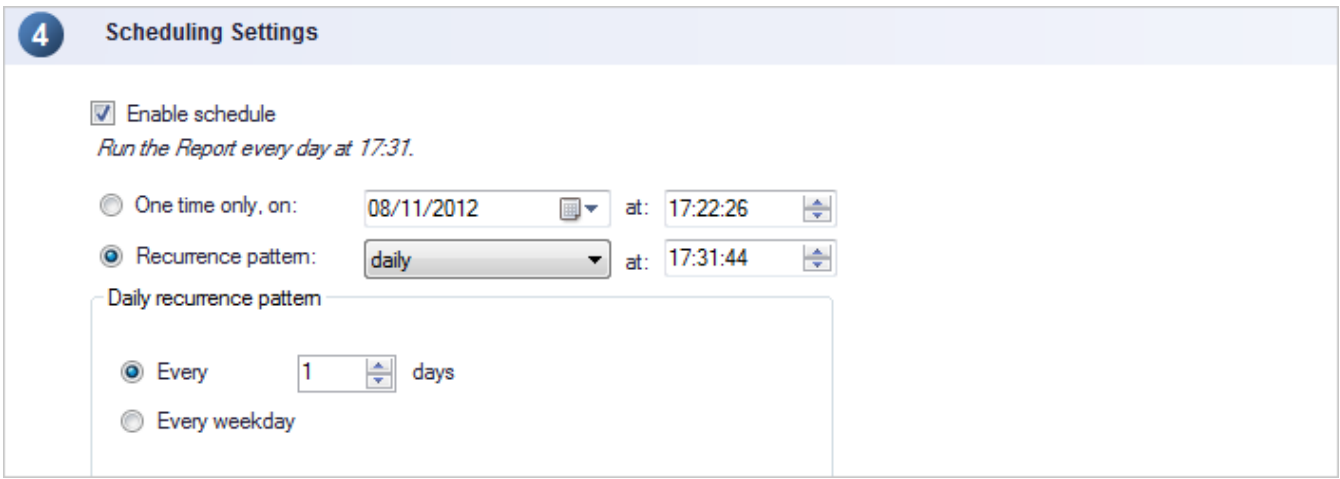
Table 69: Target Domains & Computers options

Option	Description
	From the computer tree, select a domain or workgroup and click **Add Domain**. The selected domains/work-groups are added to the report.

Option	Description
	Click **Add IP** to open the **Add IP address range** dialog. From the **Add IP address range** dialog, key in an IP range or Subnet and click **OK**.
	Select the Domain/Workgroup/IP range you want to remove and click **Remove Domain/IP**.

5. From the **Filter** drop-down menu, select a filter that you want to apply to the new scheduled report. This enables you to generate reports based on data pertaining to scan targets included in the filter.

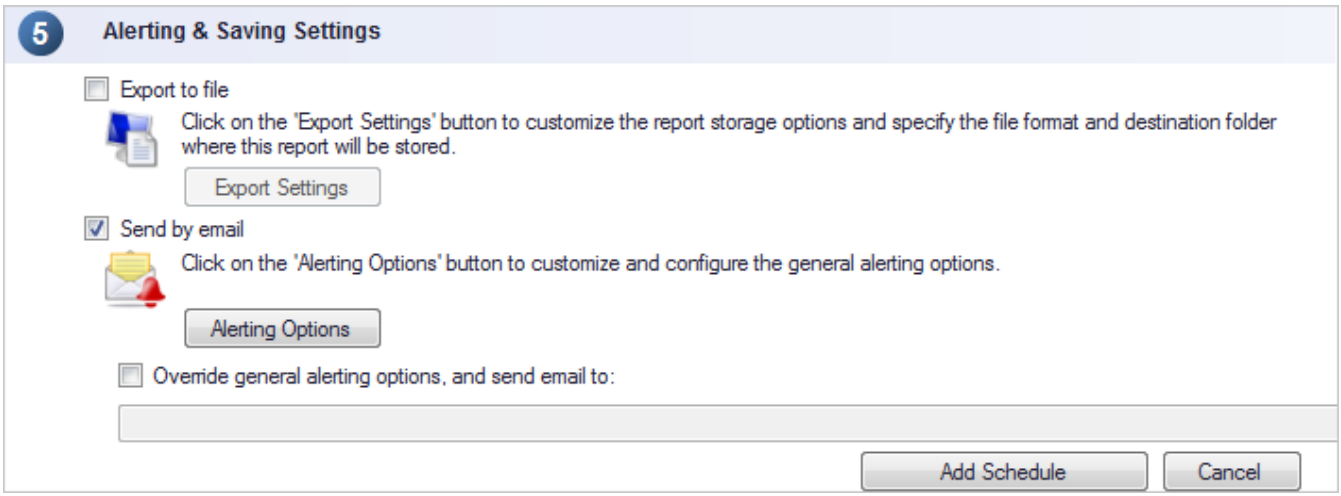
> **Note**
>
> Only custom filters can be applied to scheduled reports. For more information, refer to Using the Dashboard (page 84).



6. From **Scheduling Settings**, configure the following options:

Table 70: Scheduling options

Option	Description
Enable Schedule	Select to turn on report scheduling and generate the report according to schedule settings.
One time only, on	Specify a date and time when the report is generated. This option generates the report once, on the specified date.
Recurrence pattern	Select recurrence frequency and specify the time the scheduled report is generated.


5
Alerting & Saving Settings
Export to file
Click on the 'Export Settings' button to customize the report storage options and specify the file format and destination folder where this report will be stored.
Export Settings
Send by email
Click on the 'Alerting Options' button to customize and configure the general alerting options.
Alerting Options
Override general alerting options, and send email to:
Add Schedule
Cancel

7. From **Alerting & Saving Settings**, configure the following options:

Table 71: Alerting & Saving Settings

Option	Description
Export to file	Select to save the report in a folder.
Export Settings	Click **Export Settings** and from the **Scheduled Reports Storage Options** dialog, specify the folder where the report is saved and the format the report is saved in.
Send by email	Select to send report by email. The report is sent to recipients configured in Alerting Options.
Alerting Options	Click **Alerting Options** and configure alerts recipients and mail server settings. For more information, refer to Configuring Alerting Options (page 177).
Override general alerting options, and send email to	Select to use email recipients other than the ones configured in Alerting Options.

8. Click **Add Schedule** to save the report.

Note

10.3.2 Configuring scheduled reports options

To configure additional scheduled reports settings:

1. From the **Scheduled Reports** section, click **Scheduled Reports Options**.

2. Click **Alerting Options** to configure email settings to use to send reports. For more information, refer to Configuring Alerting Options (page 177).

3. Click **Storage Options** to specify the format and the location where generated reports are saved.

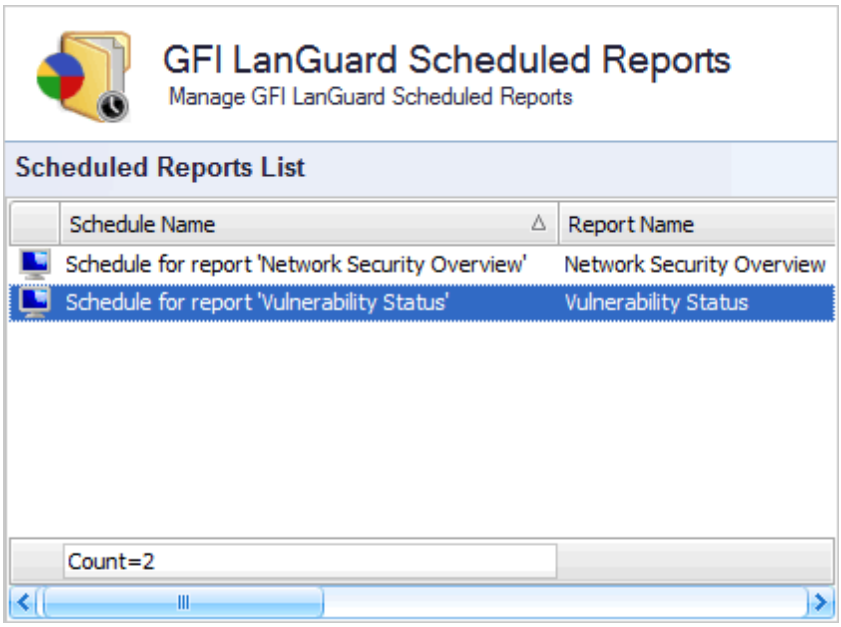
> **Note**
>
> By default, all generated reports are stored as `PDF` in: `<GFI LanGuard install directory>\Reports`.

10.3.3 Managing scheduled reports

To manage scheduled reports:

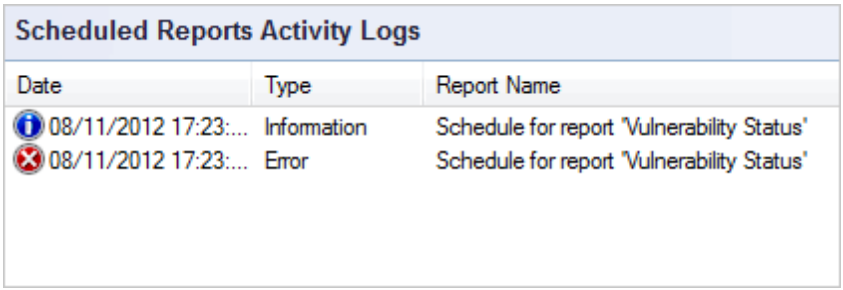
1. Click **Reports** tab.

2. From **Scheduled Reports**, click **Scheduled Reports List**.



Screenshot 111: Edit scheduled reports options

3. Double-click a report from the right pane to edit schedule report settings.



Screenshot 112: Monitor scheduled reports activity

4. Monitor schedule reports activity from the **Scheduled Reports Activity Logs** section at the bottom of the right pane.

10.4 Customizing default reports

GFI LanGuard enables you to create new reports based on the settings of an existing report. This saves you time and enables you to fine-tune existing reports, so that the data-set used to build the report precisely matches your requirements.

This section contains information about:

- Creating custom reports
- Customizing report logos
- Customizing Email Report Format

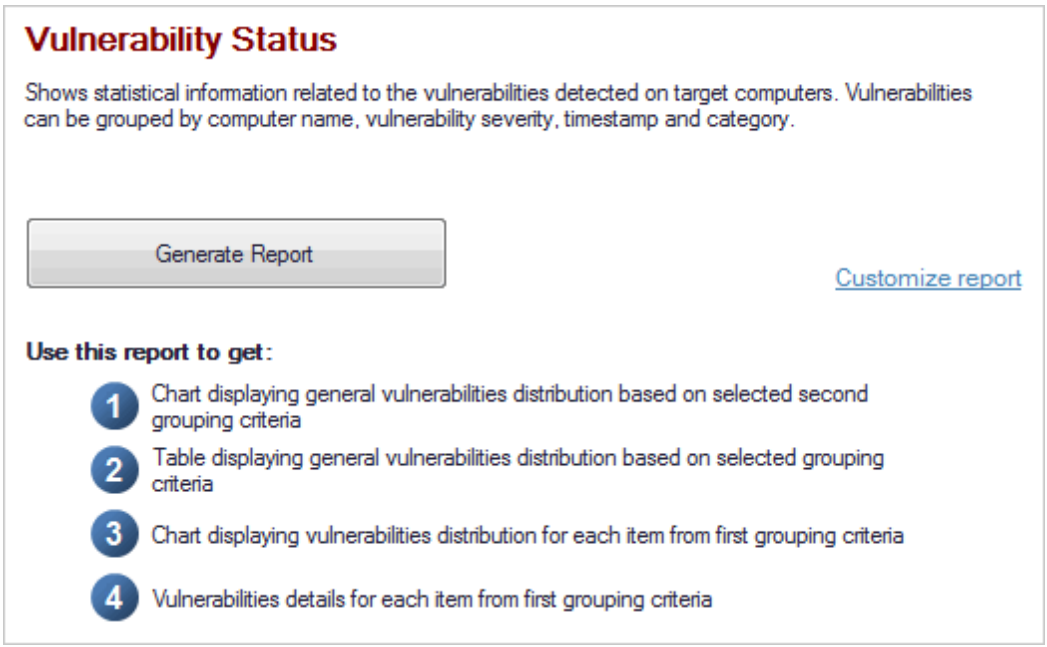
10.4.1 Creating custom reports

To create a custom report:

1. Click **Reports** tab.

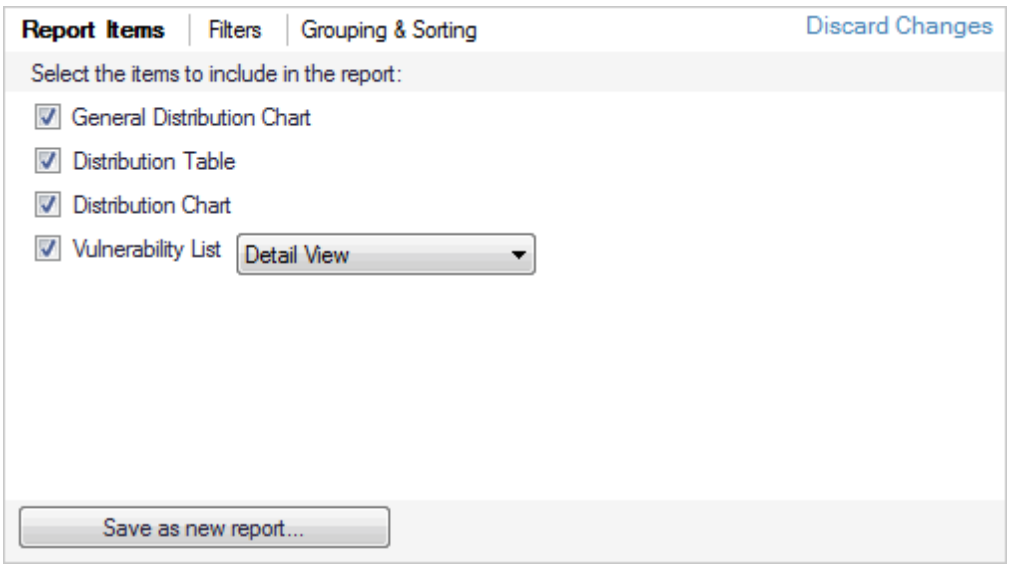
2. From the **Reports** list, select an existing report on which settings of the new reports are based on.

> **Note**
>
> Not all reports are editable.


Vulnerability Status
Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by computer name, vulnerability severity, timestamp and category.
Generate Report
Customize report
Use this report to get:
1 Chart displaying general vulnerabilities distribution based on selected second grouping criteria
2 Table displaying general vulnerabilities distribution based on selected grouping criteria
3 Chart displaying vulnerabilities distribution for each item from first grouping criteria
4 Vulnerabilities details for each item from first grouping criteria

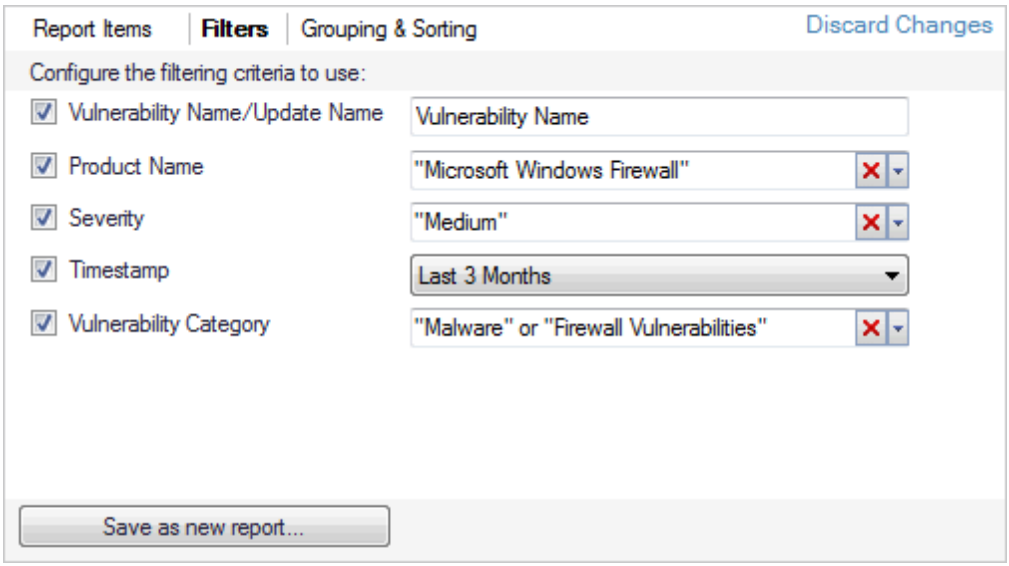
Screenshot 113: Edit report settings from the report sample preview

3. From the right pane, click **Customize report** to show advanced report options.



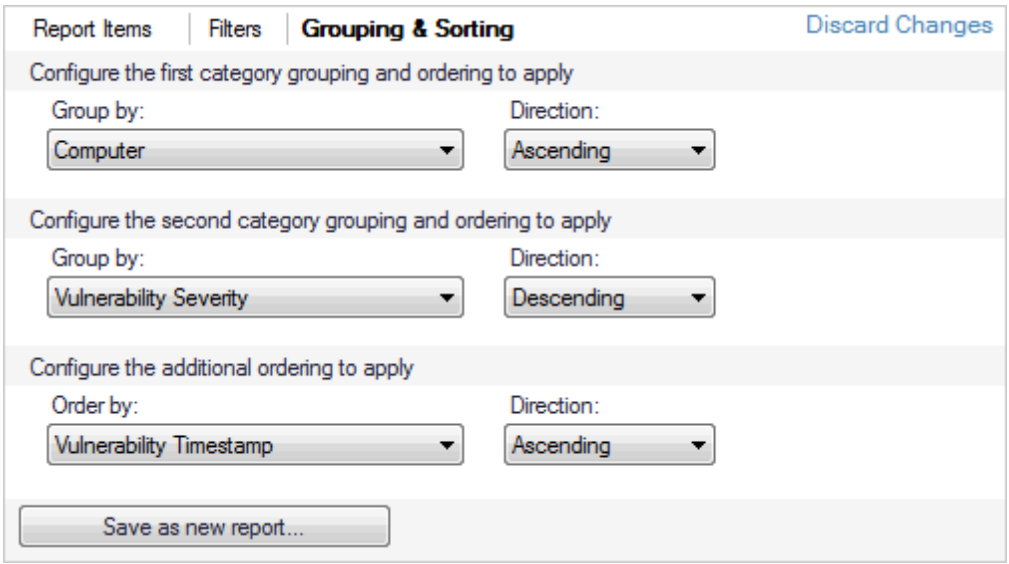
Screenshot 114: Configuring report items

4. Click **Report Items** tab and select the related items that you want to include in the report.



Screenshot 115: Configuring report filtering options

5. Click **Filters** tab and configure the available filters that relate to the report.



Screenshot 116: Configure report grouping and sorting options

6. Click **Grouping & Sorting** tab and configure:

- **First category grouping** - report information is grouped by the selected field
- **Second category grouping** - grouped information is sub-grouped by the selected field
- **Additional ordering** - order report information according to the selected field.

7. Click **Save as new report...**

8. From the **Add report** dialog, key in a name and an optional description for the new custom report. Click **OK**.

10.4.2 Customizing report logos

GFI LanGuard enables you to use your company/custom logo in the built-in reports included in the product. Logos can be placed in the header or footer sections of the report.

Customizing Report Header Logo

1. Create / select your image.

2. Resize image to: Width = **624**, Height = **25**.

3. Rename the image to **headerlogo.png**.

4. Copy / paste image in `<GFI LanGuard install directory> \ Graphics \ Logo`.

Customizing Report Footer Logo

1. Create / select your image.

2. Resize image to: Width = **109**, Height = **41**.

3. Rename the image to **footerlogo.png**.

4. Copy / paste image in `<GFI LanGuard install directory> \ Graphics \ Logo`.

10.4.3 Customizing Email Report Format

For each scheduled email report type, there is a predefined HTML format file that includes placeholders delimited with '%' symbol (for example: %TITLE%, %NAME%). You can edit the HTML format, edit HTML style, move and delete placeholders to further customize the e mail body of generated reports. The default template location is: `<GFI LanGuard install directory> \ LanGuard 11 \ Templates \ template_mailbody.xml`.

Take into consideration that GFI LanGuard can only manage known placeholders (listed below) with their predefined role. Placeholders are usable in all scheduled report types. The table below describes the customizable placeholders:

Table 72: Report placeholders

Placeholder	Description
%TITLE%	Email title for the generated report.
%NAME%	Scheduled report name.
%DESCRIPTION%:	Scheduled report description.
%TARGET%	Targets (computers, domains) represented in the scheduled report.
%LAST_RUN%	Last run date and time of the scheduled report.
%NEXT_RUN%	Next run date and time of the scheduled report. **Note** This placeholder is used only for daily digest reports.
%PROFILE%	Scanning profile used whilst running the scheduled scan. **Note** This placeholder is used only for post-scheduled scan reports.
%DURATION%	Scheduled scan duration. **Note** This placeholder is used only for post-schedules scan reports.
%ITEMS_COUNT%	Collected items count. **Note** This placeholder is used only for post-scheduled scan reports.
%AUTOREMED_MISSINGPATCHES%	Used in the report if Auto-remediate Missing Patches option is enabled for the scheduled scan. **Note** This placeholder is used only for post-scheduled scan reports.

Placeholder	Description
%AUTOREMED_MISSINGSPS%	Used in the report if Auto-remediate Missing Service Packs option is enabled for the scheduled scan. **Note** This placeholder is used only for post-scheduled scan reports.
%AUTOREMED_UNINSTAPPS%	Used in the report if Auto-remediate Uninstall Applications option is enabled for the scheduled scan. **Note** This placeholder is used only in post-scheduled scan reports.

10.5 Full text searching

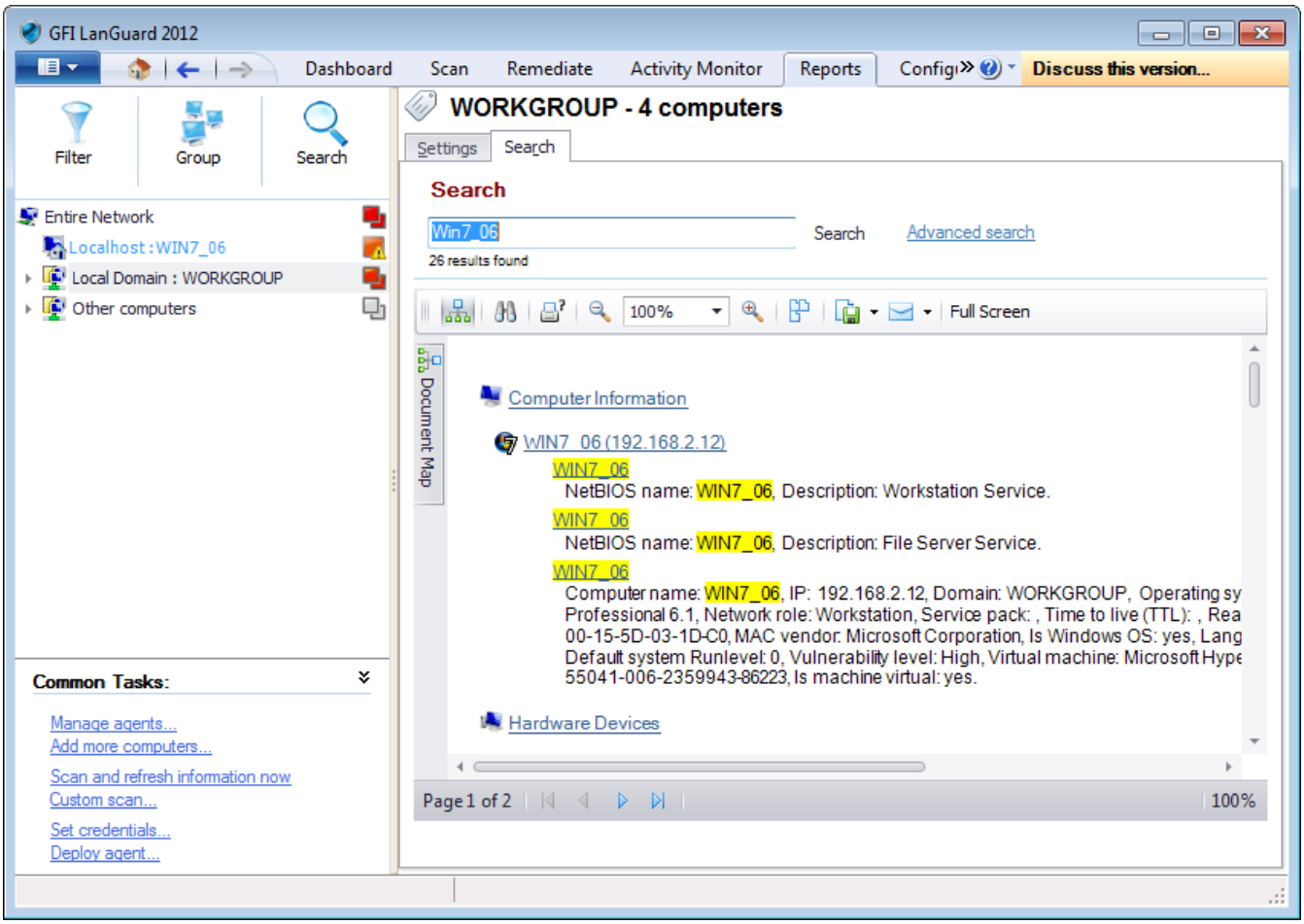
The full text search feature returns results in a structured and configurable manner. Any returned results offer clickable links for further details.

To use the full text search feature:

1. Click **Reports** tab > **Search** sub-tab.

> **Note**
>
> Search can also be accessed from **Computer tree> Search**.

2. Enter you search item and click **Search**.

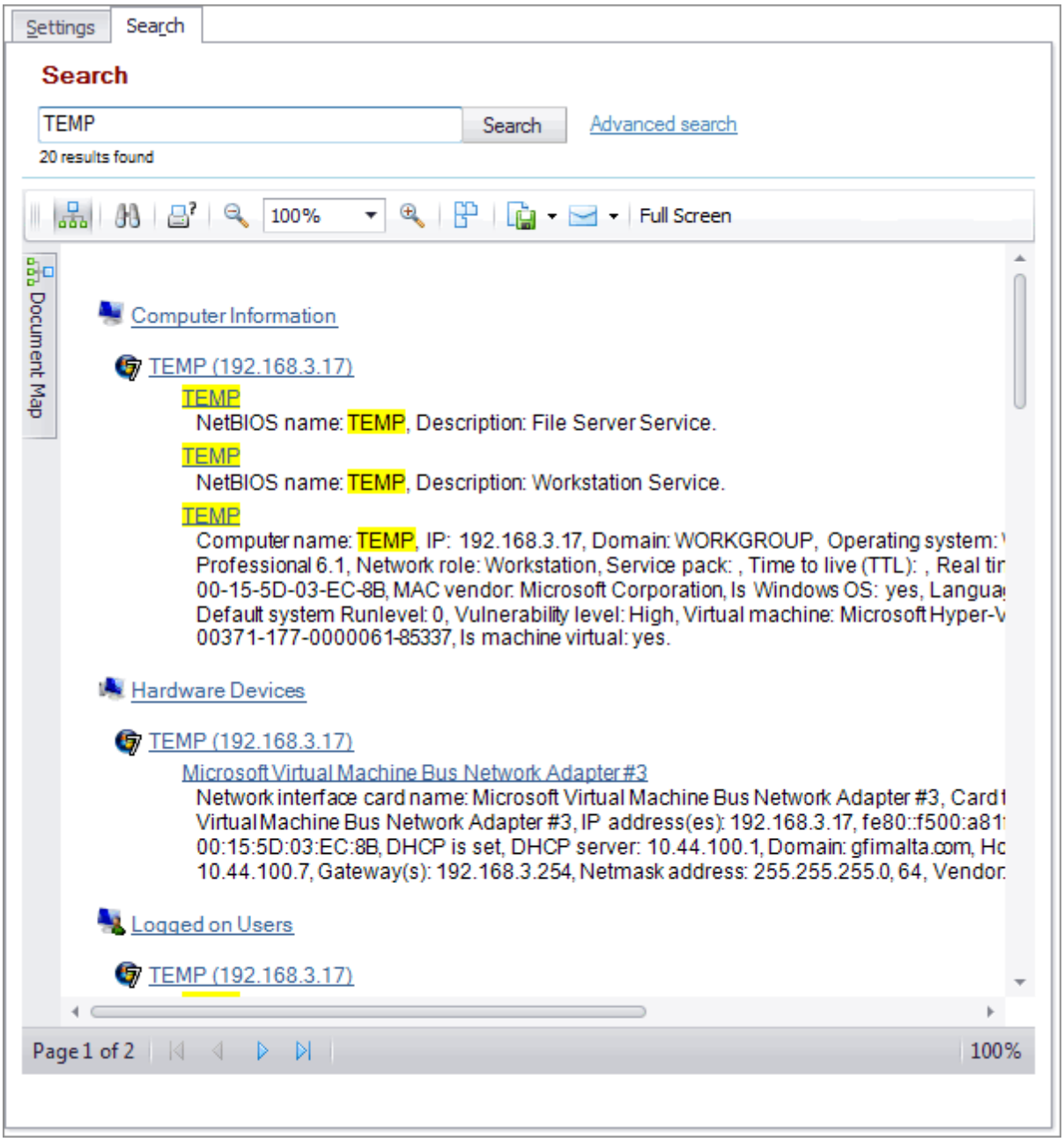


Screenshot 117: Customize the report parameters

3. (Optional) Click **Advanced search** to configure filters to narrow your search results to something more specific.

4. Analyze the search results from the results section at the bottom.

The result contains links that enable you to navigate between computers, software products and vulnerabilities. For example, you can click a missing service pack link to open the missing patches for a specific computer.


Settings
Search
Search
TEMP
Search
Advanced search
20 results found
100%
Full Screen
Document Map
Computer Information
TEMP (192.168.3.17)
TEMP
NetBIOS name: TEMP, Description: File Server Service.
TEMP
NetBIOS name: TEMP, Description: Workstation Service.
TEMP
Computer name: TEMP, IP: 192.168.3.17, Domain: WORKGROUP, Operating system:
Professional 6.1, Network role: Workstation, Service pack: , Time to live (TTL): , Real tir
00-15-5D-03-EC-8B, MAC vendor: Microsoft Corporation, Is Windows OS: yes, Langua
Default system Runlevel: 0, Vulnerability level: High, Virtual machine: Microsoft Hyper-V
00371-177-0000061-85337, Is machine virtual: yes.
Hardware Devices
TEMP (192.168.3.17)
Microsoft Virtual Machine Bus Network Adapter #3
Network interface card name: Microsoft Virtual Machine Bus Network Adapter #3, Card1
Virtual Machine Bus Network Adapter #3, IP address(es): 192.168.3.17, fe80::f500:a81
00:15:5D:03:EC:8B, DHCP is set, DHCP server: 10.44.100.1, Domain: gfimalta.com, Hc
10.44.100.7, Gateway(s): 192.168.3.254, Netmask address: 255.255.255.0, 64, Vendor:
Logged on Users
TEMP (192.168.3.17)
Page 1 of 2
100%

Screenshot 118: Navigate using report links

11 Customizing GFI LanGuard

GFI LanGuard enables you to run vulnerability scans straight out of the box – using the default settings configured prior to shipping. If required you can also customize these settings to suit any particular vulnerability management requirements that your organization might need. You can customize and configure various aspects of GFI LanGuard including scan schedules, vulnerability checks, scan filters and scan profiles.

Topics in this chapter:

11.1 Configuring Alerting Options 177

11.2 Configuring Database Maintenance Options 178

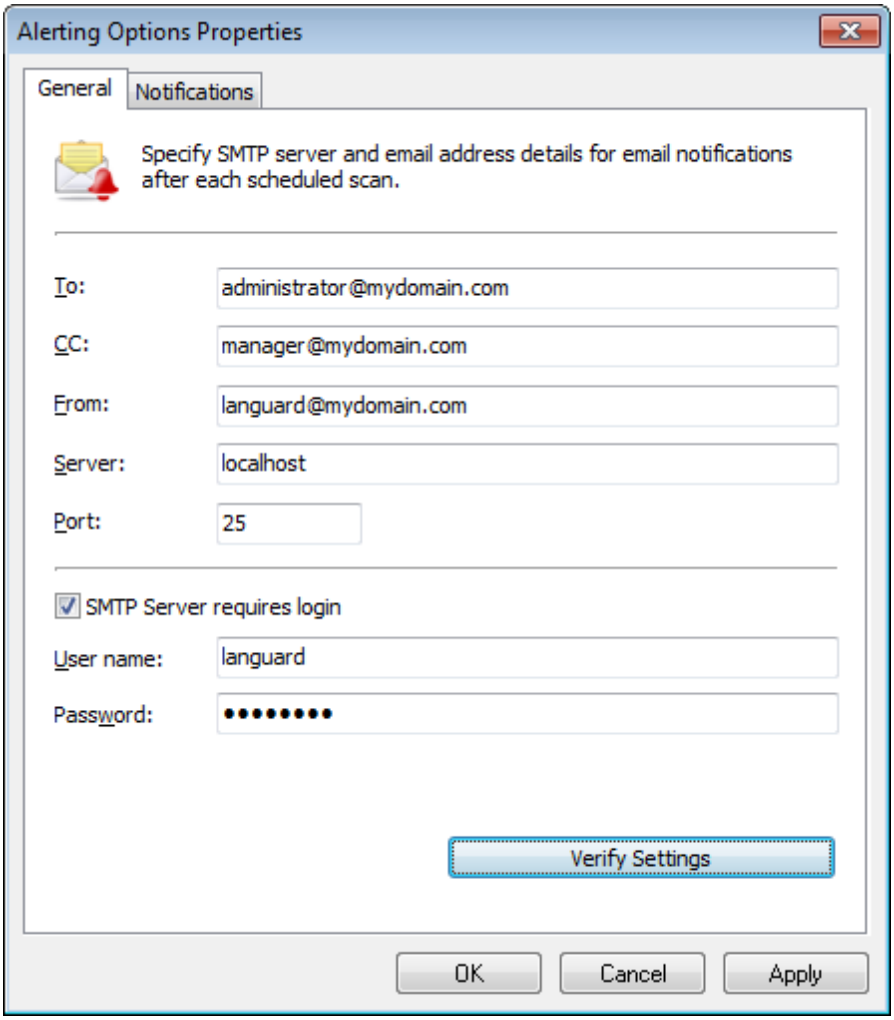
11.3 Configuring Program Updates 184

11.1 Configuring Alerting Options

To configure alerting options:

1. Click **Configuration** tab > **Alerting options**.

2. Click the link in the right pane.



Screenshot 119: Configuring Alerting Options

3. Key-in the parameters described below:

Table 73: Mail settings parameters

Option	Description
To	The recipient email address. Emails sent by GFI LanGuard are received by this email address.
CC	Key-in another email address in this field if you need to send a copy to another email address.
From	The sender email address. GFI LanGuard will use this email account to send the required emails.
Server	Defines the server through which emails are routed. This can be either an FQDN (Fully Qualified Domain Name) or an IP Address.
Port	Defines the IP port through which emails are routed. Default value is 25
SMTP Server requires login	Select this option if the SMTP server requires a username and password to authenticate.

4. Click on the **Verify Settings** button to verify email settings.

5. Select **Notifications** and configure the following options:

Table 74: Notifications options

Option	Description
Enable daily digest	Receive daily report with all changes made on the entire network. Configure the time when the daily digest email is received.
Report format	Specify the report format received by email.
Send an email on new product news	Receive an email containing new product news.

6. Click **OK**.

11.2 Configuring Database Maintenance Options

GFI LanGuard ships with a set of database maintenance options through which you can maintain your scan results database backend in good shape.

For example, you can improve product performance and prevent your scan results database backend from getting excessively large by automatically deleting scan results that are older than a specific number of months.

If you are using an Access™ database backend, you can also schedule database compaction. Compaction enables you to repair any corrupted data and to delete database records marked for deletion in your database backend; ensuring the integrity of your scan results database. The following sections provide you with information about:

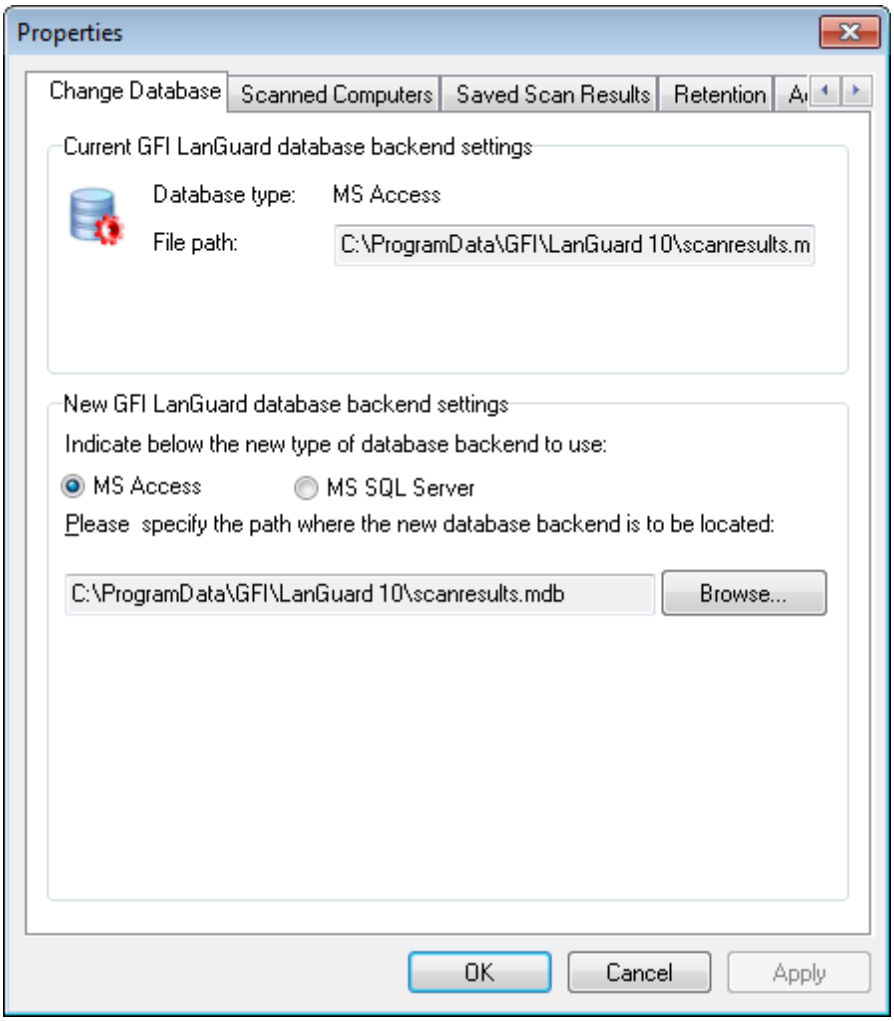
- Using Access™ as a database backend
- Using SQL Server® as a database backend
- Managing saved scan results
- List scanned computers
- Configure advanced database maintenance options
- Configure database retention options

11.2.1 Using Access™ as a database backend

GFI LanGuard supports both Access™ and SQL Server® (2000 or higher) based database backend.

To store scan results in an Access™ database:

1. Click **Configuration** tab > **Database Maintenance Options** > **Database backend settings**.



Screenshot 120: The database maintenance properties dialog

2. Select the **MS Access** option and specify the full path (including the file name) of your Access™ database backend.

> **Note**
>
> The specified database file is created if it does not exist.

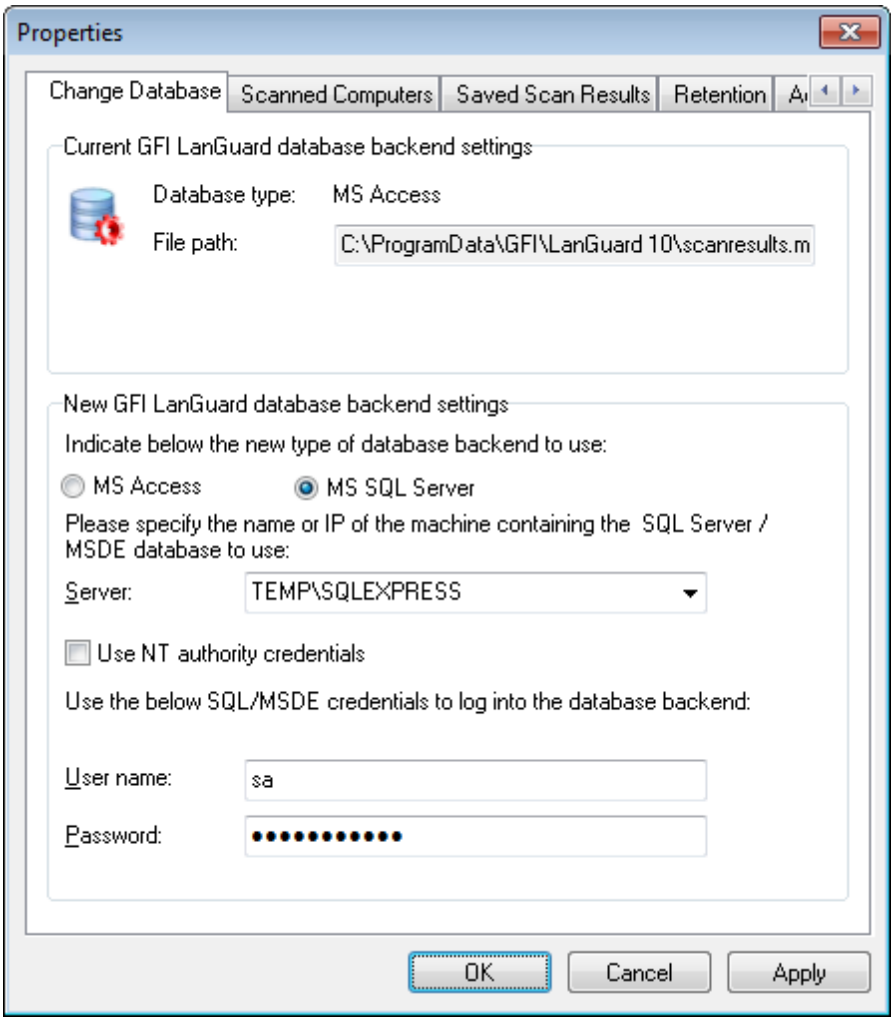
> **Note**
>
> If the specified database file already exists and belongs to a previous version of GFI LanGuard, you are asked to over-write the existing information.

3. Click **OK**.

11.2.2 Using SQL Server® as a database backend

To store scan results in an SQL Server® database:

1. Click **Configuration** tab > **Database Maintenance Options** > **Database backend settings**.



Screenshot 121: SQL Server® database backend options

2. Select the **MS SQL Server** option and choose the SQL Server that will be hosting the database from the provided list of servers discovered on your network.

3. Specify the SQL Server credentials or select the **Use NT authority credentials** option to authenticate to the SQL server using windows account details.

4. Click **OK** to finalize your settings.

Note

If the specified server and credentials are correct, GFI LanGuard will automatically log on to your SQL Server and create the necessary database tables. If the database tables already exist, it will re-use them.

Note

When using NT authority credentials, make sure that GFI LanGuard services are running under an account that has both access and administrative privileges on the SQL Server databases.

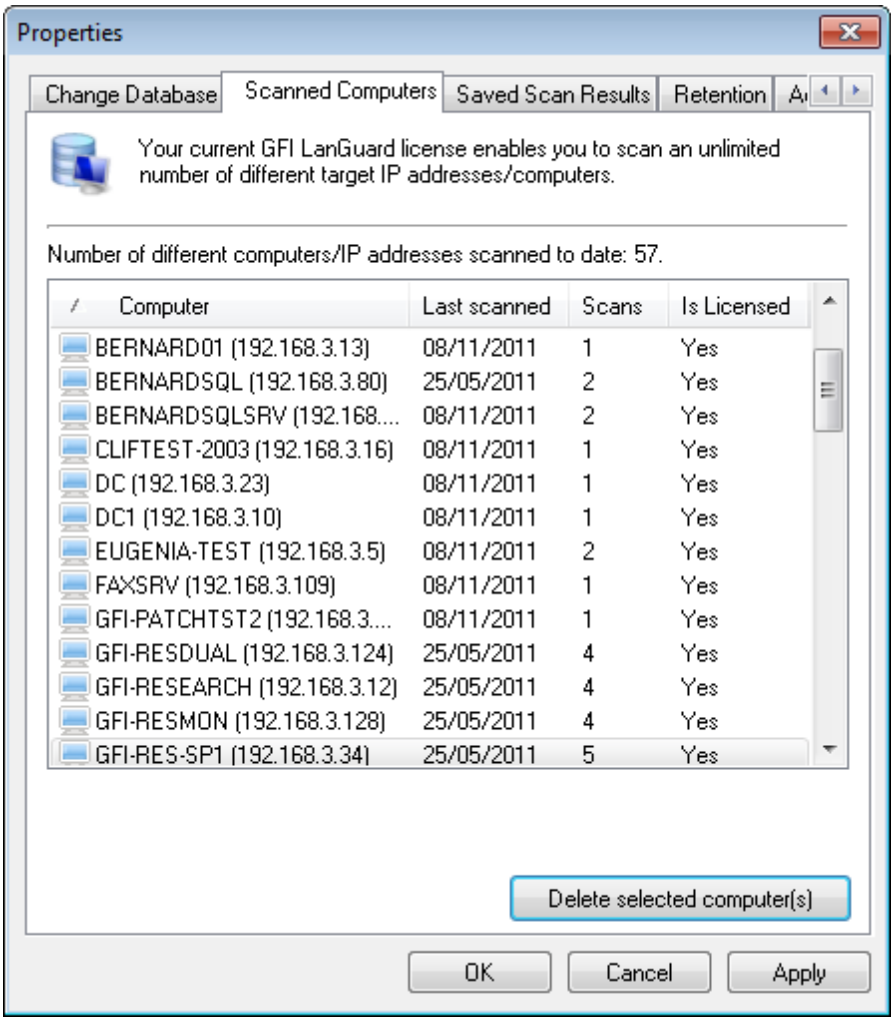
5. Click **Yes** to stop all current scans.

6. If the current Access™ database contains data, click **OK** to transfer all scan data to the SQL Server® database.

11.2.3 Managing saved scan results

Use the **Saved Scan Results** tab to maintain your database backend and delete saved scan results that are no longer required. Deletion of non-required saved scan results can be achieved manually as well as automatically through scheduled database maintenance.

During scheduled database maintenance, GFI LanGuard automatically deletes saved scan results that are older than a specific number of days/weeks or months. You can also configure automated database maintenance to retain only a specific number of recent scan results for every scan target and scan profile.


Properties
Change Database
Scanned Computers
Saved Scan Results
Retention
Your current GFI LanGuard license enables you to scan an unlimited number of different target IP addresses/computers.
Number of different computers/IP addresses scanned to date: 57.
Computer
Last scanned
Scans
Is Licensed
BERNARD01 (192.168.3.13) 08/11/2011 1 Yes
BERNARDSQL (192.168.3.80) 25/05/2011 2 Yes
BERNARDSQLSRV (192.168.... 08/11/2011 2 Yes
CLIFTEST-2003 (192.168.3.16) 08/11/2011 1 Yes
DC (192.168.3.23) 08/11/2011 1 Yes
DC1 (192.168.3.10) 08/11/2011 1 Yes
EUGENIA-TEST (192.168.3.5) 08/11/2011 2 Yes
FAXSRV (192.168.3.109) 08/11/2011 1 Yes
GFI-PATCHTST2 (192.168.3.... 08/11/2011 1 Yes
GFI-RESDUAL (192.168.3.124) 25/05/2011 4 Yes
GFI-RESEARCH (192.168.3.12) 25/05/2011 4 Yes
GFI-RESMON (192.168.3.128) 25/05/2011 4 Yes
GFI-RES-SP1 (192.168.3.34) 25/05/2011 5 Yes
Delete selected computer(s)
OK
Cancel
Apply

Screenshot 122: Database maintenance properties: Managed saved scan results tab

To manage saved scan results:

1. Click on the **Configuration** tab **> Database Maintenance Options > Manage saved scan results**.

2. To delete saved scan results, select the particular result(s) and click **Delete Scan(s)**.

3. To let GFI LanGuard manage database maintenance for you, select **Scans generated during the last** to delete scan results, which are older than a specific number of days/weeks, or months or **Scans per scan target per profile in number of** to retain only a specific number of recent scan results.

11.2.4 List scanned computers

GFI LanGuard maintains a global list of scanned computers for licensing purposes. Any computers in excess of what is specified in the licensing information are not scanned.

GFI LanGuard enables systems administrators to delete scanned computers in order to release licenses that were previously utilized.

To delete computers previously scanned:

1. Click **Configuration** tab **> Database Maintenance Options > Manage list of scanned computers**.

2. Select the computers to delete and click **Delete selected computer(s)**.

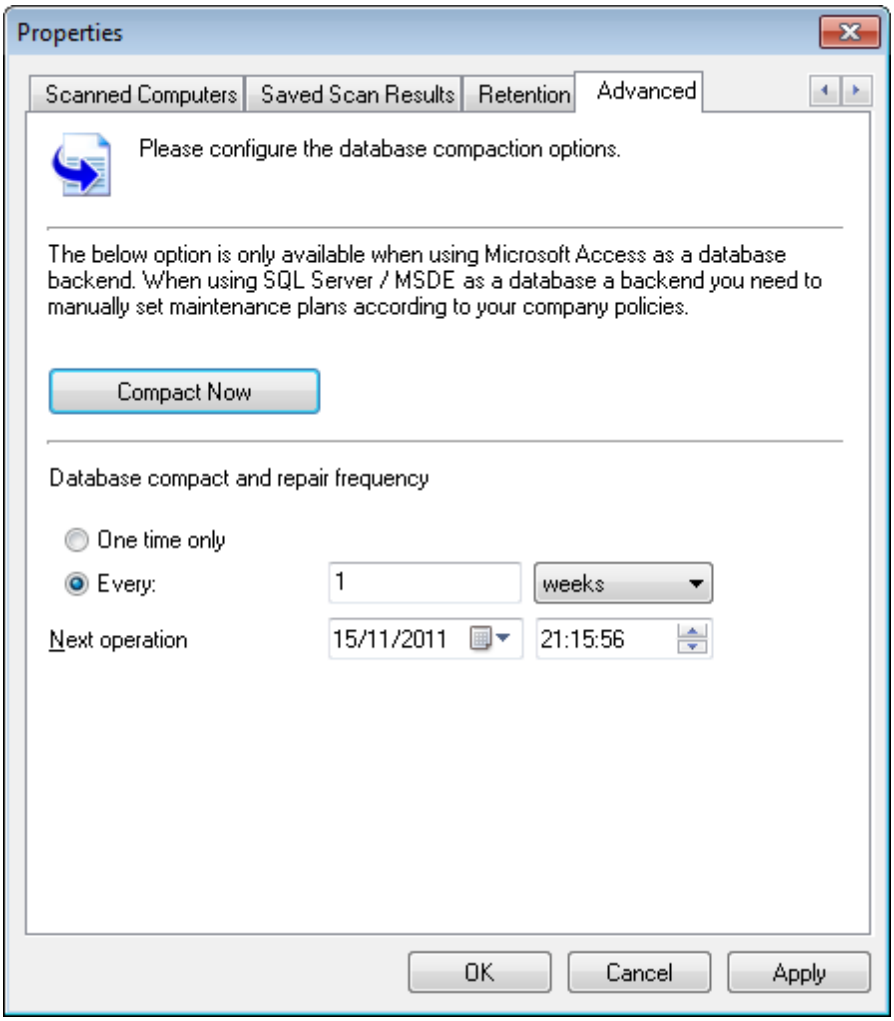
IMPORTANT

Deleting computers from the database is a one-way operation that will also delete all computer related data from the database. Once deleted, this data is no longer available.

11.2.5 Configure advanced database maintenance options

GFI LanGuard enables you to repair and compact the Access™ database backend automatically to improve performance.

During compaction, the database files are reorganized and records that have been marked for deletion are removed. In this way, you can regain used storage space. During this process, GFI LanGuard also repairs corrupted database backend files. Corruption may occur for various reasons. In most cases, a Access™ database is corrupted when the database is unexpectedly closed before records are saved (for example, due to a power failure, unresponsive operations forced reboots, and so on).



Screenshot 123: Database Maintenance properties: Advanced tab

To compact and repair a Access™ database backend:

1. Click **Configuration** tab > **Database Maintenance Options** > **Database maintenance plan**.

2. To manually launch a repair and compact process on an Access™ database backend, click **Compact Now**.

3. To automate the repair and compact process on an Access™ database backend select:

- **One time only** - to schedule a onetime Access™ database repair and compact
- **Every** - to execute a repair and compact process on a regular schedule.

Specify the date, time and frequency in days/weeks or months at which the compact and repair operations will be executed on your database backend.

11.2.6 Configure database retention options

Database retention options enable you to keep your database clean and consistent, by configuring GFI LanGuard to automatically delete unwanted scan results and scan history information while retaining important ones.

To configure retention settings:

1. Click **Configuration** tab > **Database Maintenance Options** > **Database backend settings** > **Retention** tab.

2. Configure the options described below:

Table 75: Database retention options

Option	Description
Keep scans generated during the last	Keep scan results generated during the specified number of days/weeks/months.
Keep scans per scan target per profile number of	Specify the number of scan results to keep, for every scan target by every scan profile.
Never delete history	Select this option if you want to keep all scan history.
Keep history for the last	Keep scan history for the specified number of days/weeks/months.

3. Click **OK**.

11.3 Configuring Program Updates

This tool enables GFI LanGuard to detect the latest vulnerabilities and maintain its scanning performance. Configure GFI LanGuard to auto-download updates released by GFI to improve functionalities in GFI LanGuard. These updates also include checking GFI web site for newer builds. Updates can be enabled/disabled by selecting the checkbox in the **Auto-download** column.

GFI LanGuard can download all Unicode languages. This includes (but is not limited to) English, German, French, Italian, Spanish, Arabic, Danish, Czech, Finnish, Hebrew, Hungarian, Japanese, Korean, Dutch, Norwegian, Polish, Portuguese, Portuguese/Brazilian, Russian, Swedish, Chinese, Chinese (Taiwan), Greek, and Turkish.

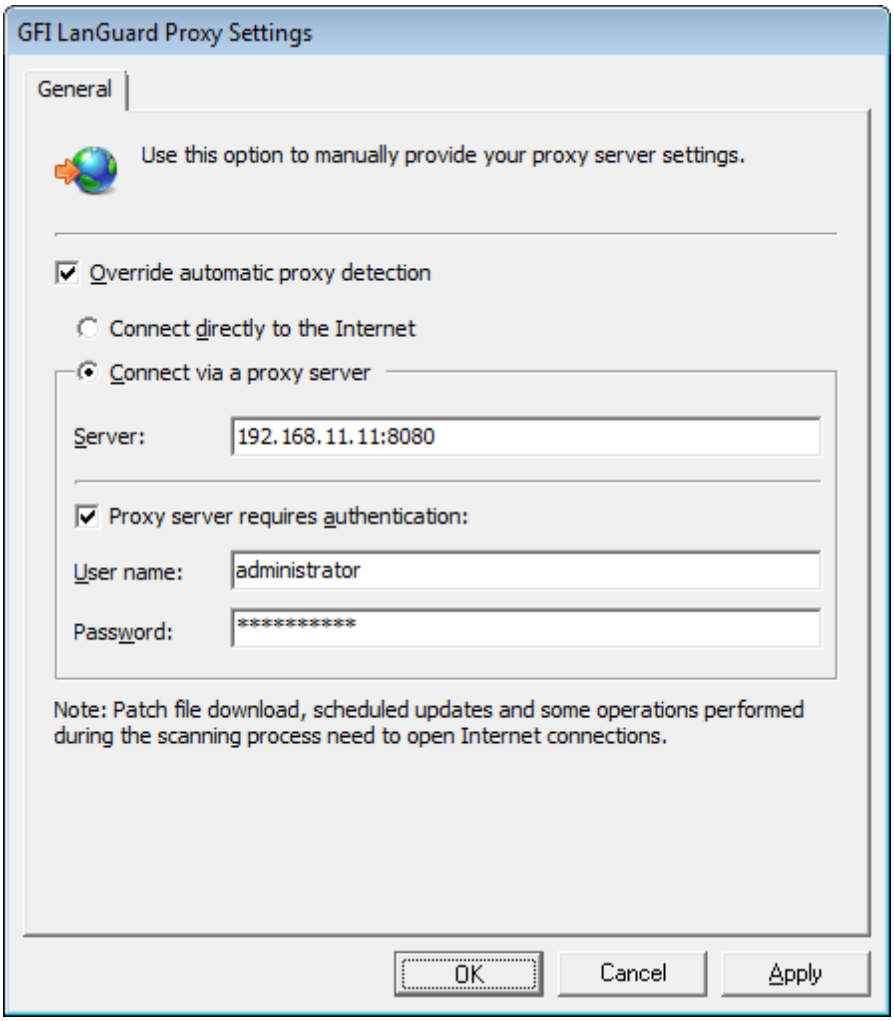
The following sections provide you with information about:

- Configuring proxy settings
- Configuring auto-update options
- Installing program updates manually

11.3.1 Configuring proxy settings

To manually configure proxy server settings for Internet updates:

1. Click on **Configuration** tab > **Program Updates**.
2. From **Common Tasks** select **Edit proxy settings**.



Screenshot 124: Configuring proxy server settings

3. Select **Override automatic proxy detection;** configure the options described below:

Table 76: Proxy settings

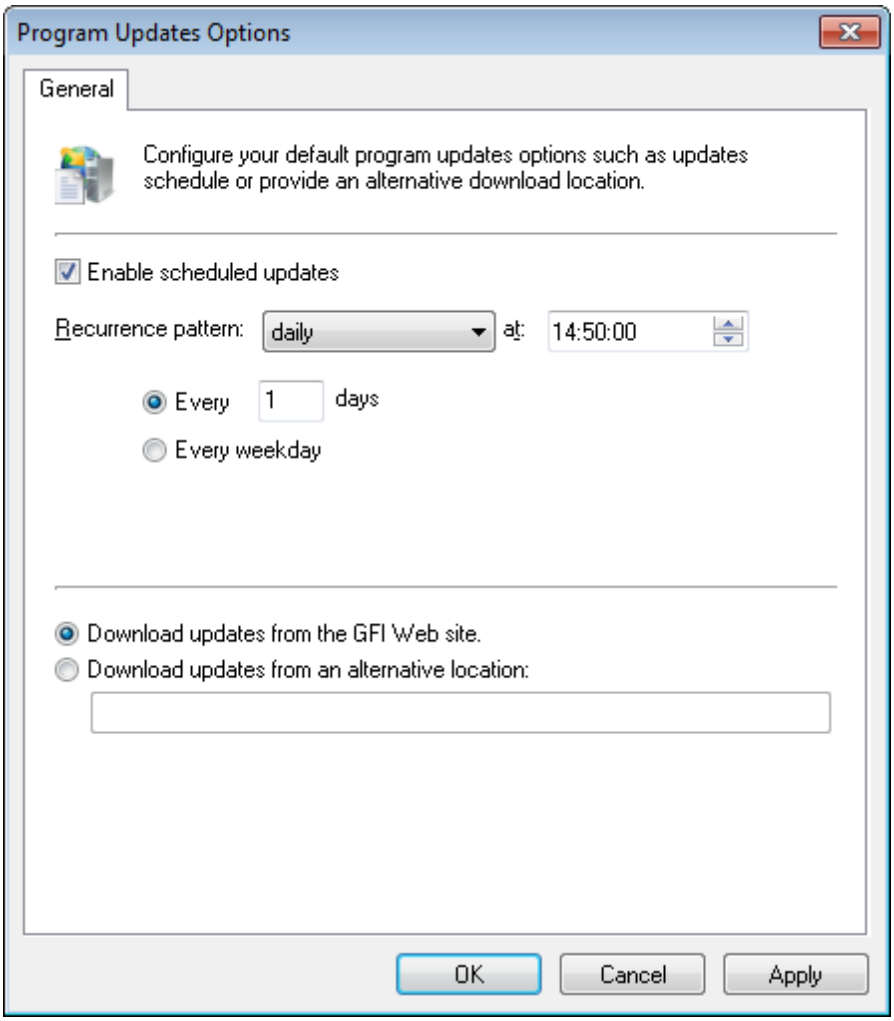
Option	Description
Connect directly to the Internet	A direct Internet connection is available.
Connect via a proxy server	Internet access is through a proxy server. Update the Server name and port number using this format <server>:<port>
Proxy server requires authentication	(Optional) Enter username and password if required by the proxy server.

4. Click **OK**.

11.3.2 Configuring auto-update options

GFI LanGuard can check for the availability of software updates at every program startup. To disable/enable this feature

1. Click on **Configuration** tab **> Program Updates**. From **Common Tasks** select **Edit program updates options**.



Screenshot 125: Configure updates at application startup

2. Select/unselect **Check for updates at application startup** to enable/disable auto update checks at application startup.

3. Select/unselect enable scheduled updates to configure the frequency of update checks.

4. Specify whether GFI LanGuard download updates from GFI website or from an alternative location.

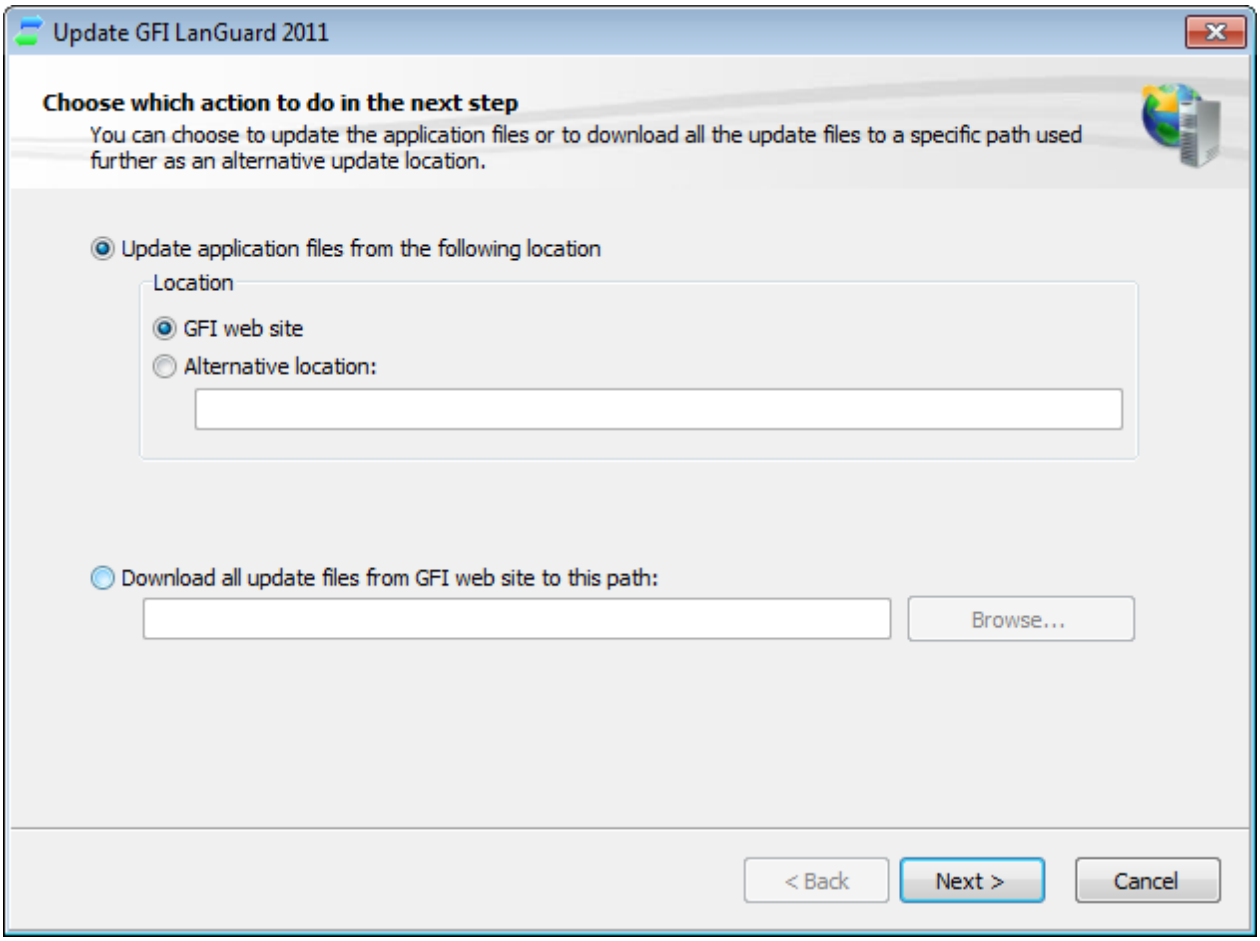
5. Click **OK**.

11.3.3 Installing program updates manually

To start GFI LanGuard program updates manually:

1. Click on **Configuration** tab > **Program Updates**.

2. From **Common Tasks** click **Check for updates**.


Update GFI LanGuard 2011
Choose which action to do in the next step
You can choose to update the application files or to download all the update files to a specific path used further as an alternative update location.
Update application files from the following location
Location
GFI web site
Alternative location:
Download all update files from GFI web site to this path:
Browse...
< Back
Next >
Cancel

Screenshot 126: Check for Updates wizard

3. Specify the location from where the required update files will be downloaded.

4. (Optional) Change the default download path, select **Download all update files…** to this path to provide an alternate download path to store all GFI LanGuard updates.

5. Click **Next** to proceed with the update.

6. Select the updates and click **Next**.

7. Click **Start** to start the update process.

12 Scanning Profile Editor

The scanning profiles that ship with GFI LanGuard are already pre-configured to run a number of vulnerability checks on selected target. You can however disable vulnerability scanning as well as customize the list of vulnerability checks executed during a scan. Scans can be modified through the **Scanning Profile Editor**.

Topics in this chapter:

12.1 Create a new Scanning Profile 188

12.2 Configuring Vulnerabilities 189

12.3 Configuring Patches 199

12.4 Configuring Network & Software Audit options 202

12.5 Configuring security scanning options 209

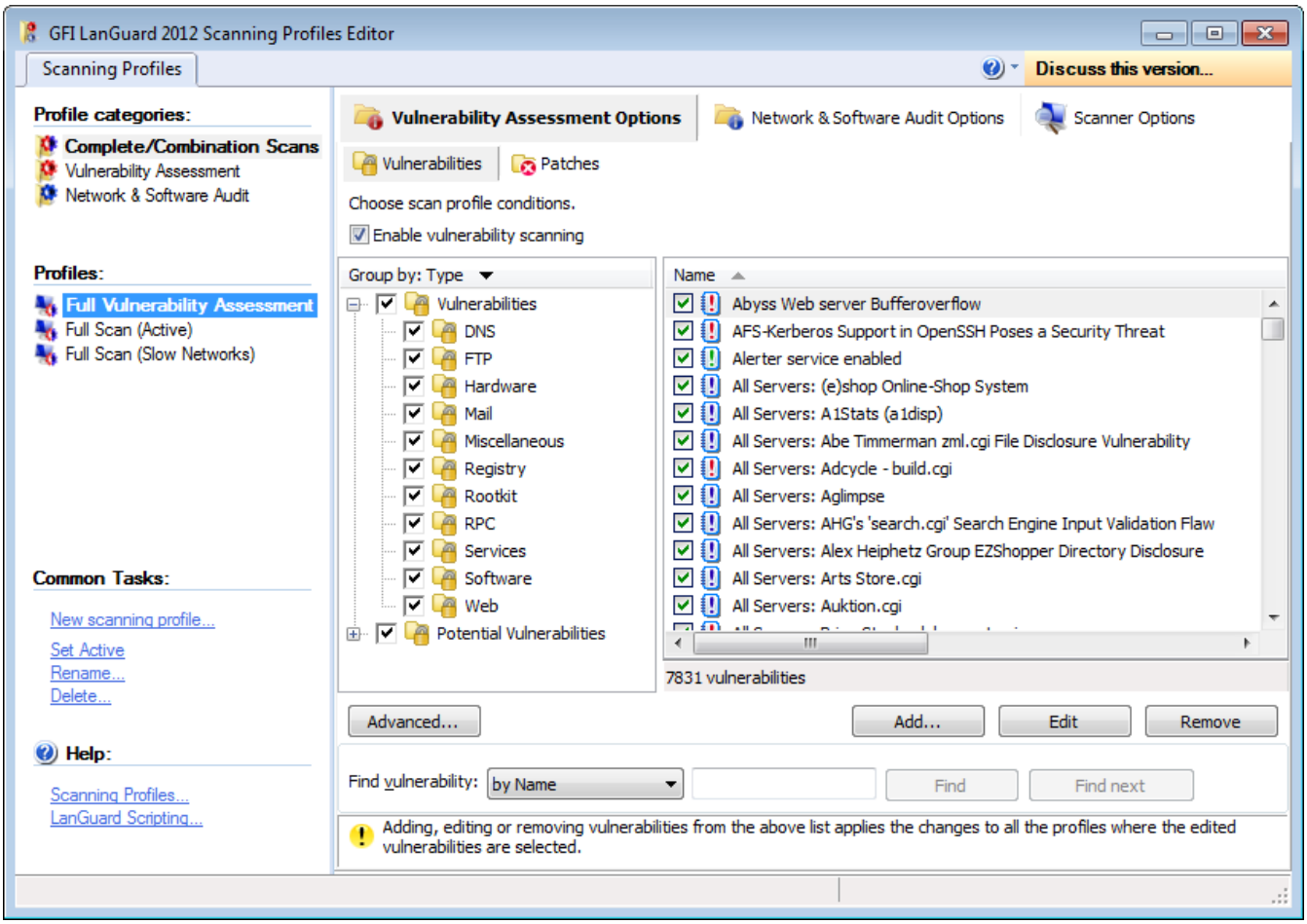
12.1 Create a new Scanning Profile

The **Scanning Profiles Editor** enables you to create new scanning profiles. To create a new custom scanning profile:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

3. In **Scanning Profiles Editor** from **Common Tasks**, click **New scanning profile**.



Screenshot 127: The Scanning Profile Editor

4. Specify the name of the new profile and optionally select **Copy all settings from an existing profile** to clone settings from an existing profile.

5. Click **OK** to save settings. The new scanning profile is added under **Profiles** in the left pane.

12.2 Configuring Vulnerabilities

The **Vulnerability Assessment Options** tab enables you to configure which Microsoft®/non-Microsoft® and Security/non-Security updates are checked when scanning targets with the selected profile.

The following sections provide you with information about:

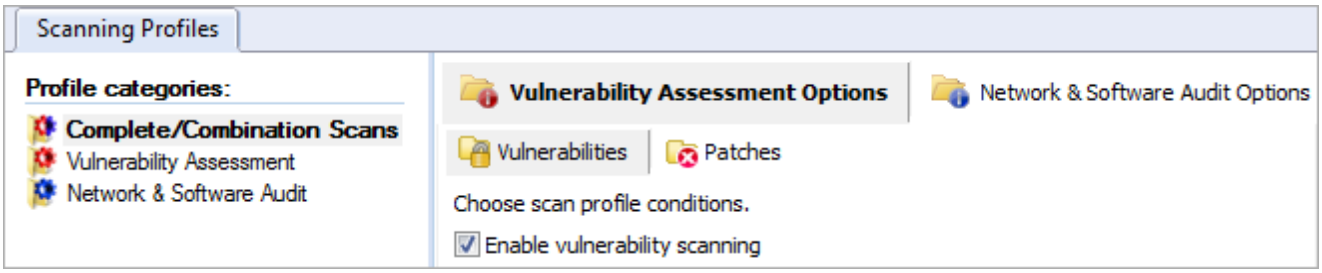
- Enabling vulnerability scanning
- Customizing the list of vulnerabilities to be scanned
- Customizing vulnerability checks properties
- Setting up vulnerability check conditions

12.2.1 Enabling vulnerability scanning

To enable vulnerability scanning:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.



Screenshot 128: Enabling vulnerability scanning for the selected scanning profile

3. From the **Vulnerability Assessment Options** tab, click **Vulnerabilities** sub-tab.

4. Select the scanning profile to customize from the left pane under **Profiles**.

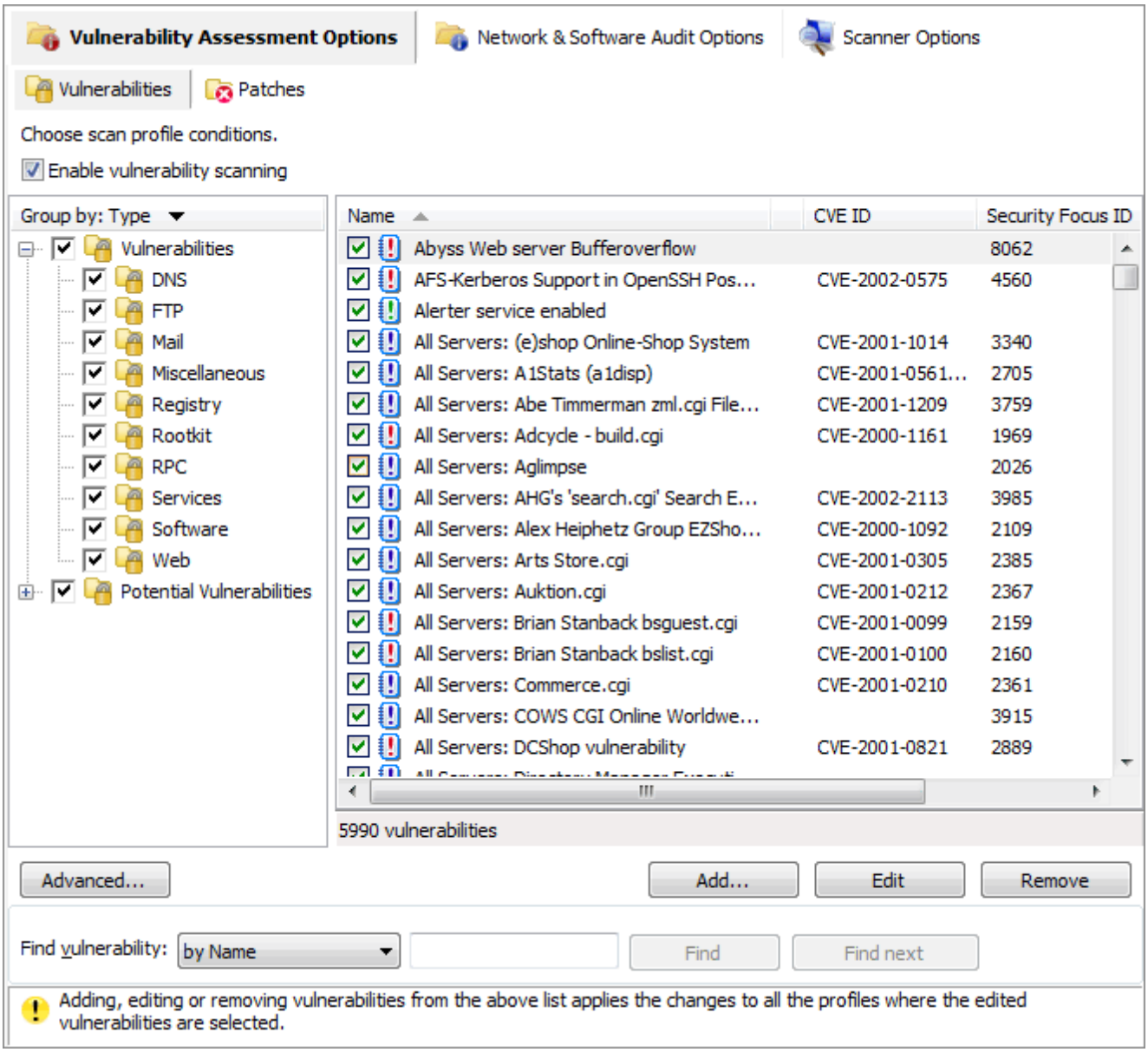
5. In the right pane, select **Enable Vulnerability Scanning**.

> **Note**
>
> Vulnerability scanning is configured on a scan profile by scan profile basis. If in a particular profile this option is not selected, no vulnerability tests will be performed in the security audits carried out by this scanning profile.

12.2.2 Customizing the list of vulnerabilities to be scanned

To specify which vulnerabilities will be enumerated and processed by a scanning profile during a security audit:

1. From **Vulnerability Assessment Options** tab, select the scanning profile to customize from the left pane under **Profiles**.

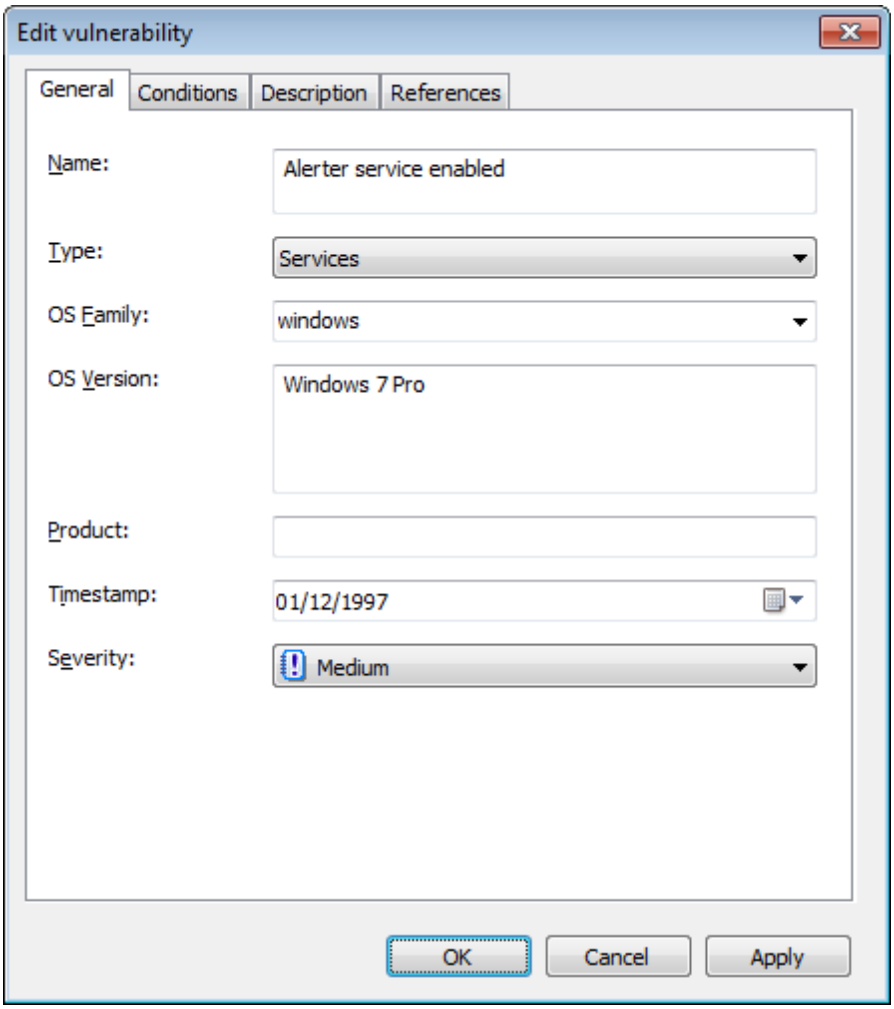


Screenshot 129: Select the vulnerability checks to be run by this scanning profile

2. In the right pane, select the vulnerability checks to execute through this scanning profile.

12.2.3 Customizing vulnerability checks properties

All the checks listed in the **Vulnerabilities** tab have specific properties that determine when the check is triggered and what details will be enumerated during a scan.



Screenshot 130: Vulnerability properties dialog: General tab

To change the properties of a vulnerability check:

1. Right-click on the vulnerability to customize, select **Properties**.

2. Customize the selected vulnerability check from the tabs described below:

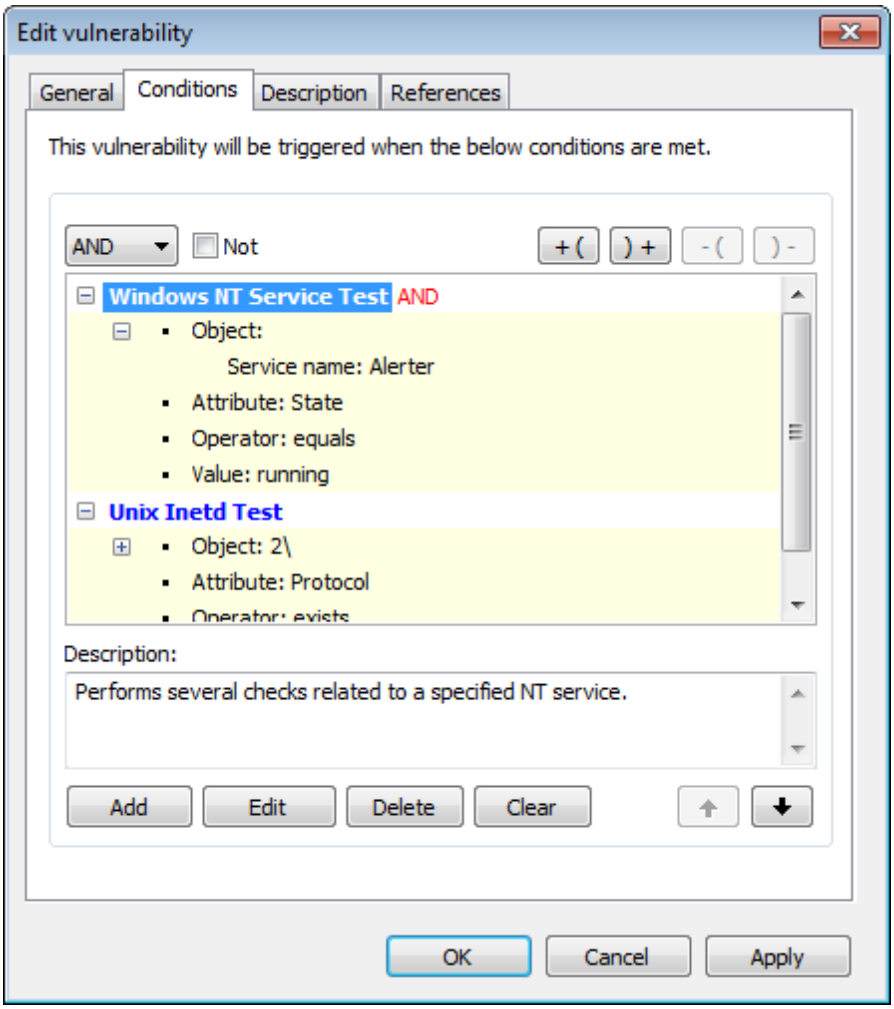
Table 77: Vulnerability properties dialog

Tab	Description
General	Use this tab to customize the general details of a vulnerability check including vulnerability check name, vulnerability type, OS family, OS version, Product, Timestamp and Severity.
Conditions	Use this tab to configure the operational parameters of this vulnerability check. These parameters will define whether a vulnerability check is successful or not.
Description	Use this tab to customize the vulnerability check description.
References	Use this tab to customize references and links that lead to relevant information in the OVAL, CVE, MS Security, Security Focus and SANS TOP 20 reports.

3. Click on **OK** to save your settings.

12.2.4 Setting up vulnerability check conditions

The **Conditions** tab enables you to add or customize conditions, which define whether the computer or network being scanned is vulnerable, or not. It is therefore of paramount importance that any custom checks defined in this section are set-up by qualified personnel that are aware of the ramifications of their actions.

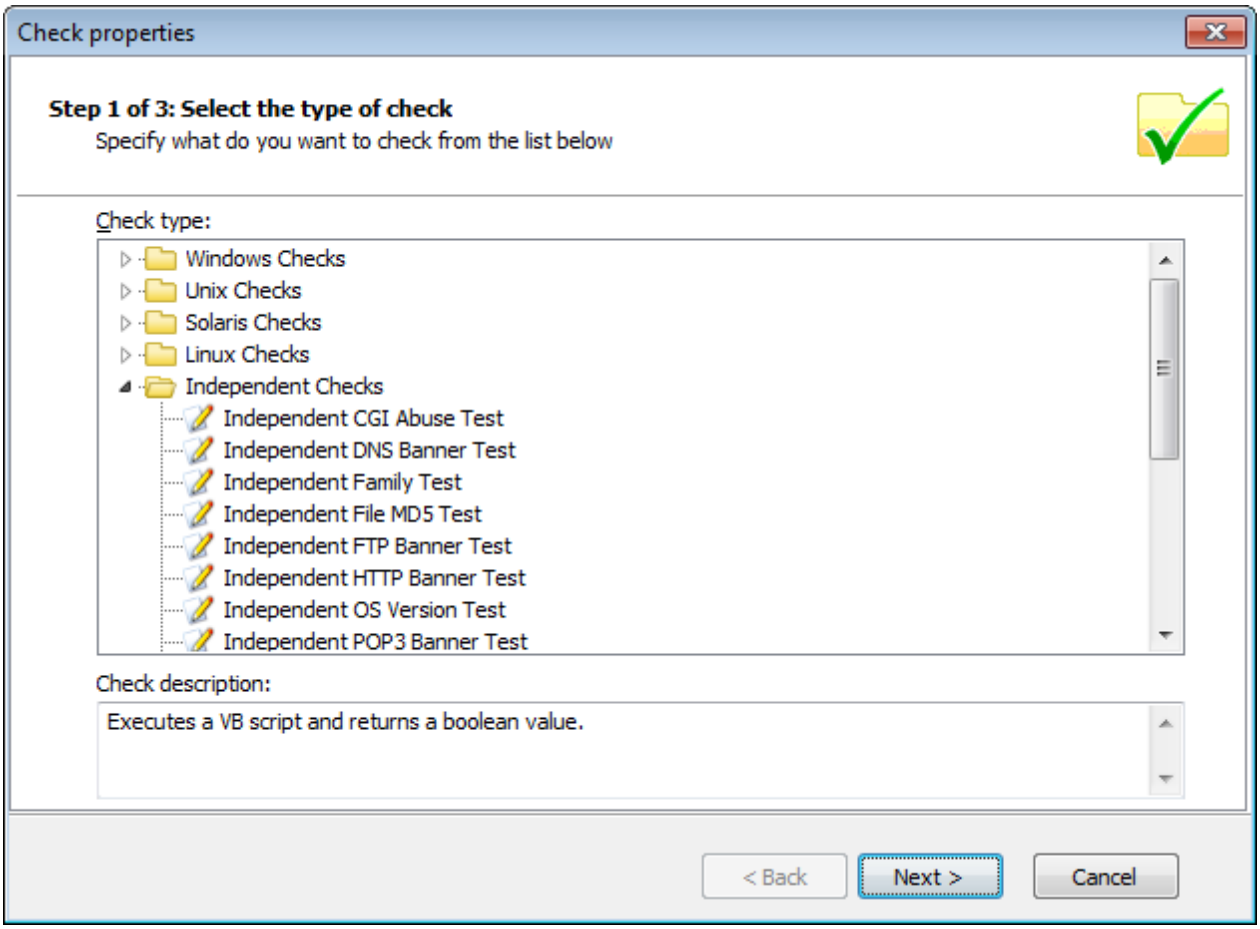


Screenshot 131: Vulnerability conditions setup tab

To add a vulnerability check condition:

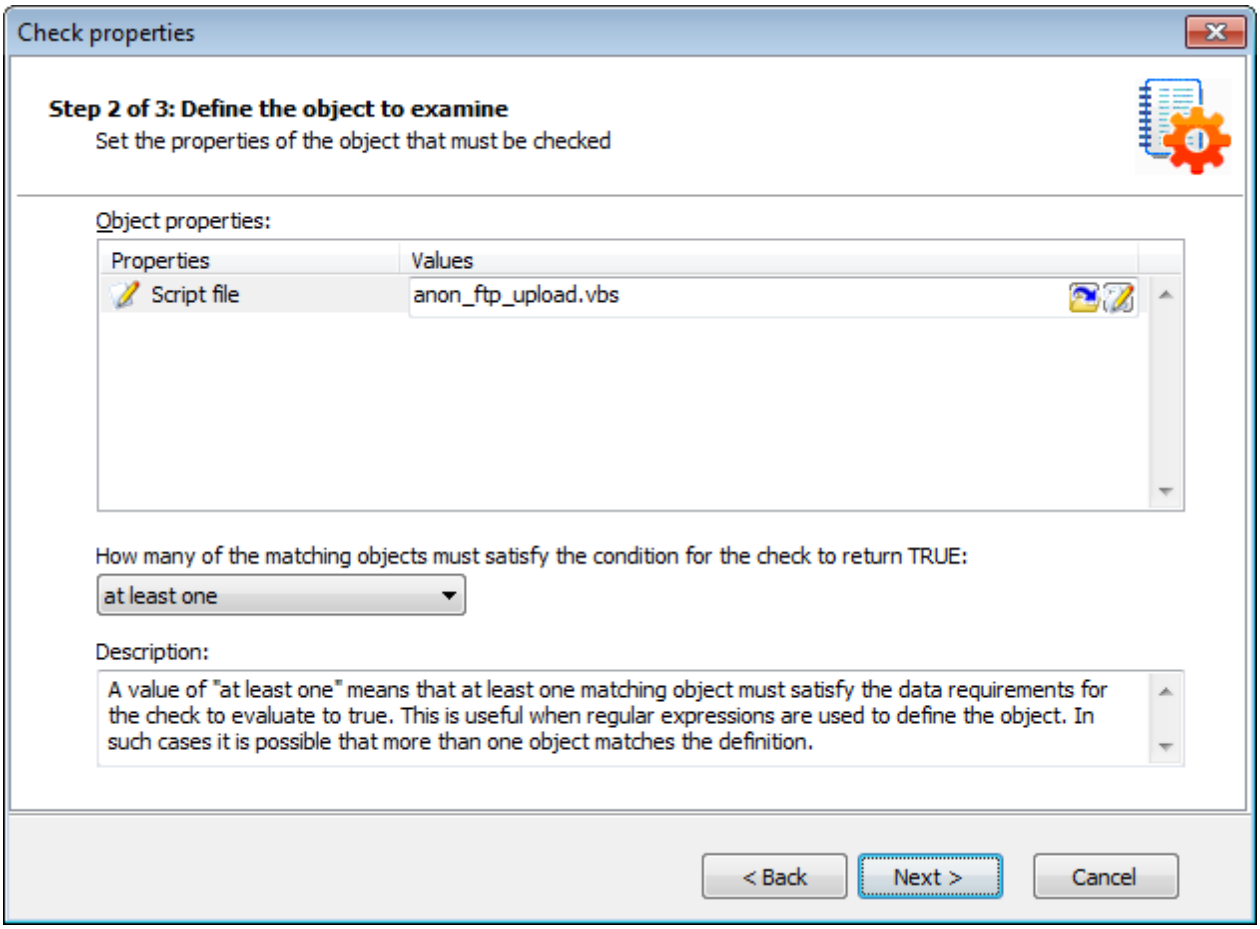
1. From **Vulnerability Assessment Options** tab > **Vulnerabilities** sub-tab, right-click a vulnerability from the list of vulnerabilities and select **Properties**.

2. From the **Edit vulnerability** dialog, click **Conditions** tab > **Add**.



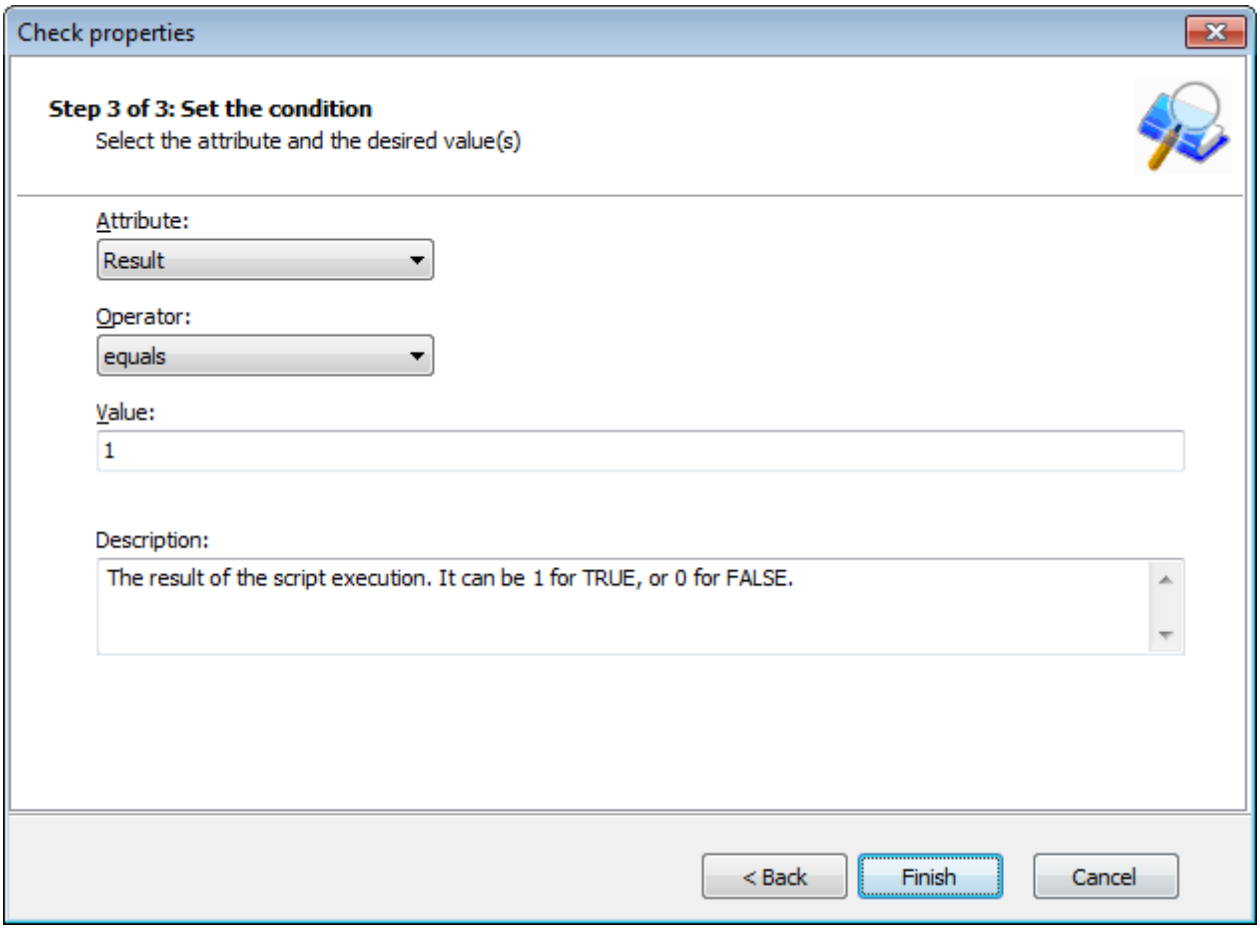
Screenshot 132: Check properties wizard - Select check type

3. Select the type of check to be configured and click **Next**.


Check properties
Step 2 of 3: Define the object to examine
Set the properties of the object that must be checked
Object properties:
Properties
Values
Script file
anon_ftp_upload.vbs
How many of the matching objects must satisfy the condition for the check to return TRUE:
at least one
Description:
A value of "at least one" means that at least one matching object must satisfy the data requirements for the check to evaluate to true. This is useful when regular expressions are used to define the object. In such cases it is possible that more than one object matches the definition.
< Back
Next >
Cancel

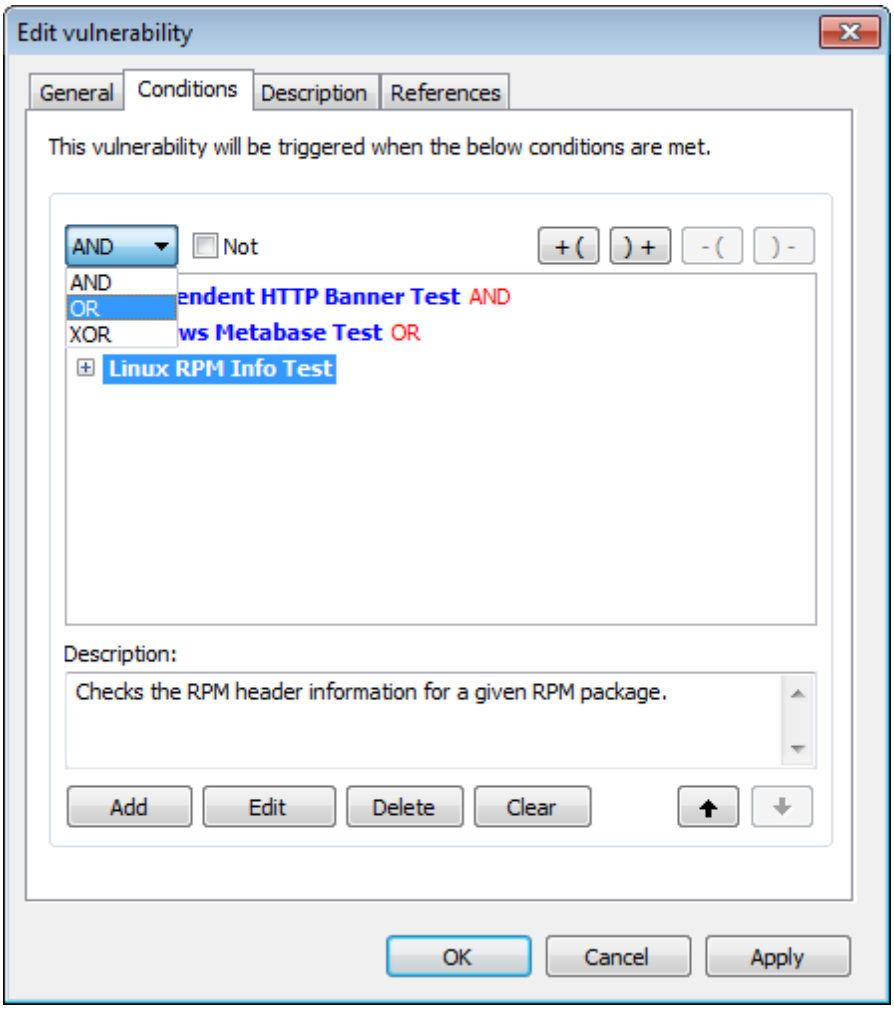
Screenshot 133: Check properties wizard - Define the object to examine

4. Define the object to examine and click **Next**.



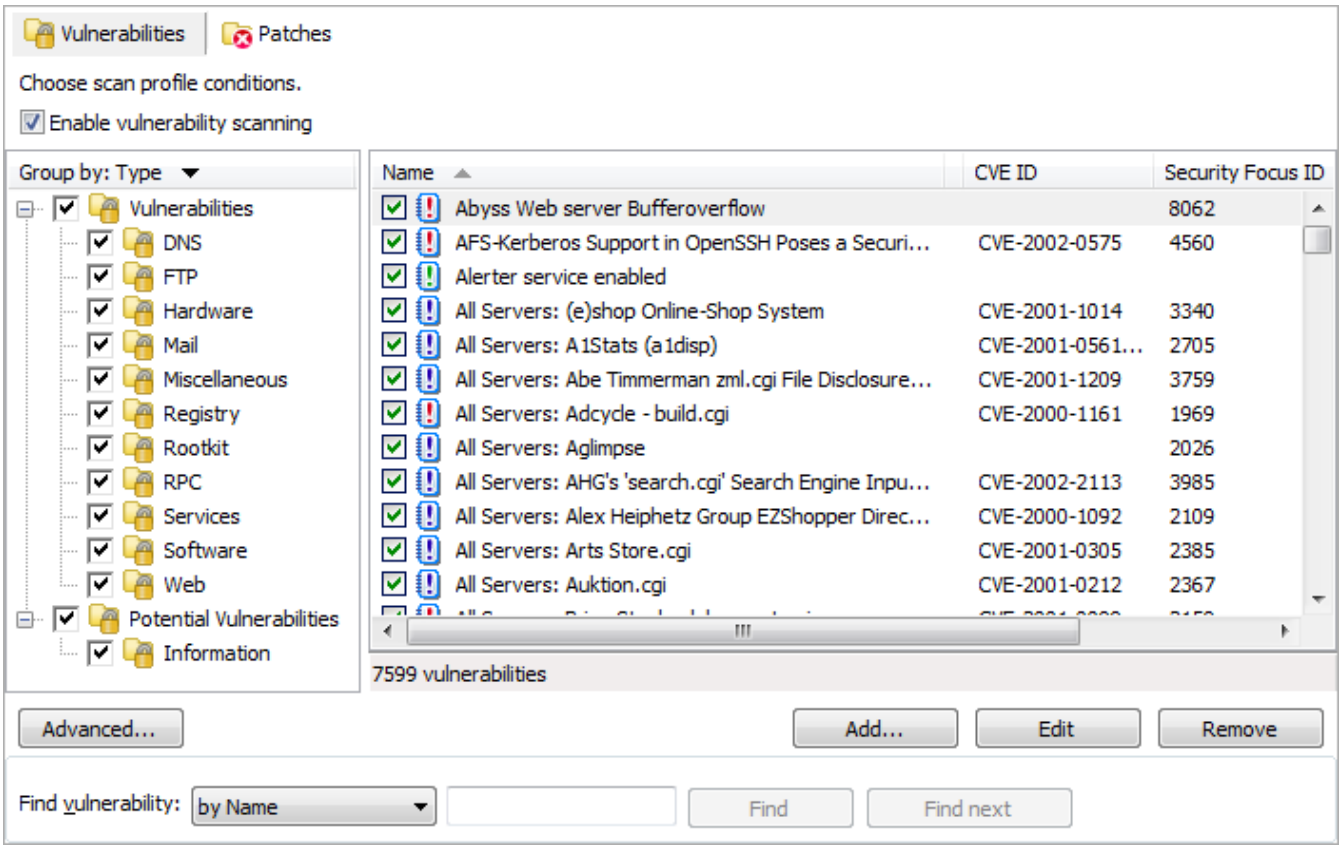
Screenshot 134: Check properties wizard - Set required conditions

5. Specify required conditions and click **Finish** to finalize your settings.



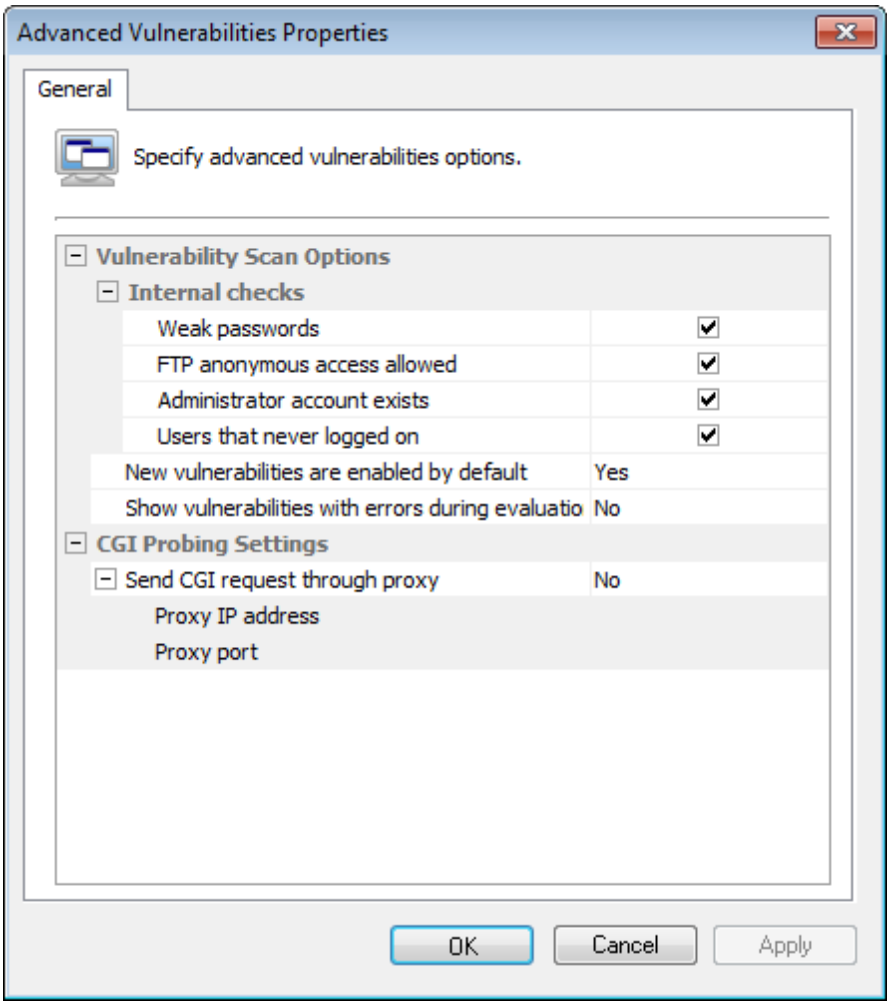
Screenshot 135: Check properties wizard - Defining conditional operators

6. If more than one condition is set up, define conditional operators and click **OK** to finalize your configuration settings.



Screenshot 136: Advanced vulnerability options

7. (Optional) Click **Advanced** in the **Vulnerabilities** tab to launch the advanced vulnerabilities scanning options.



Screenshot 137: Advanced vulnerability scanning dialogs

The options in **Advanced Vulnerabilities Options** are used to:

- Configure extended vulnerability scanning features that check your target computers for weak passwords, anonymous FTP access, and unused user accounts.
- Configure how GFI LanGuard handles newly created vulnerability checks.
- Configure GFI LanGuard to send CGI requests through a specific proxy server. This is mandatory when CGI requests will be sent from a computer that is behind a firewall to a target web server that is 'outside' the firewall. For example, Web servers on a DMZ.

The firewall will generally block all the CGI requests that are directly sent by GFI LanGuard to a target computer that is in front of the firewall. To avoid this, set the **Send CGI requests through proxy** option to 'Yes' and specify the name/IP address of your proxy server and the communication port which will be used to convey the CGI request to the target.

12.3 Configuring Patches

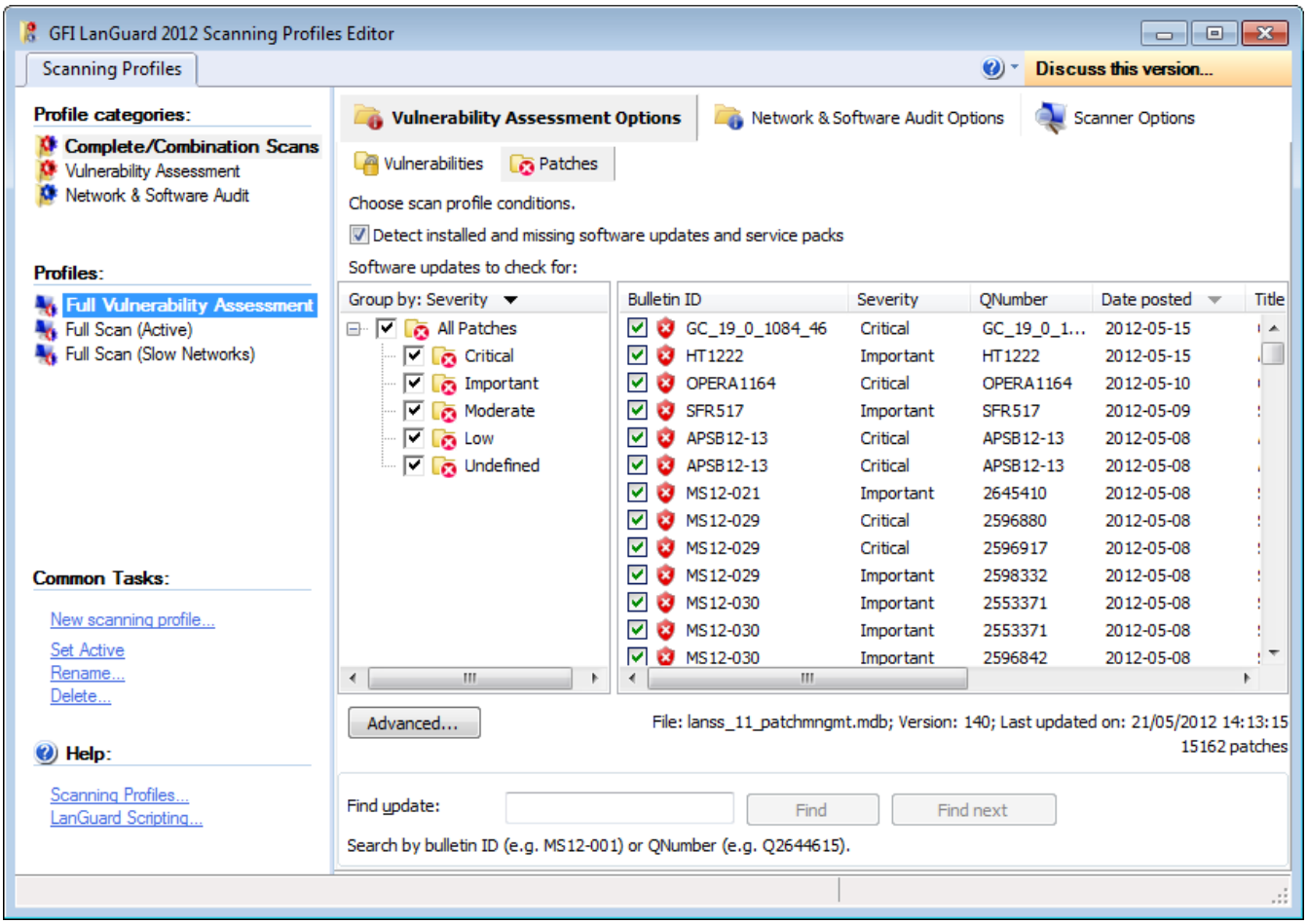
The **Patches** tab specifies the security updates checked during vulnerability scanning. The patches checked are selected from the complete list of supported software updates, included in this tab. This list is automatically updated whenever GFI releases a new GFI LanGuard missing patch definition file.

The following sections contain information about:

- Enabling/disabling missing patch detection checks
- Customizing the list of software patches to scan

» Searching for Bulletin Information

12.3.1 Enabling/disabling missing patch detection checks



Screenshot 138: Scanning Profiles properties: Patches tab options

To enable missing patch detection checks in a particular scanning profile:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

3. From the **Vulnerability Assessment Options** tab, click **Patches** sub-tab.

4. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

5. In the right pane, select **Detect installed and missing service packs/patches** option.

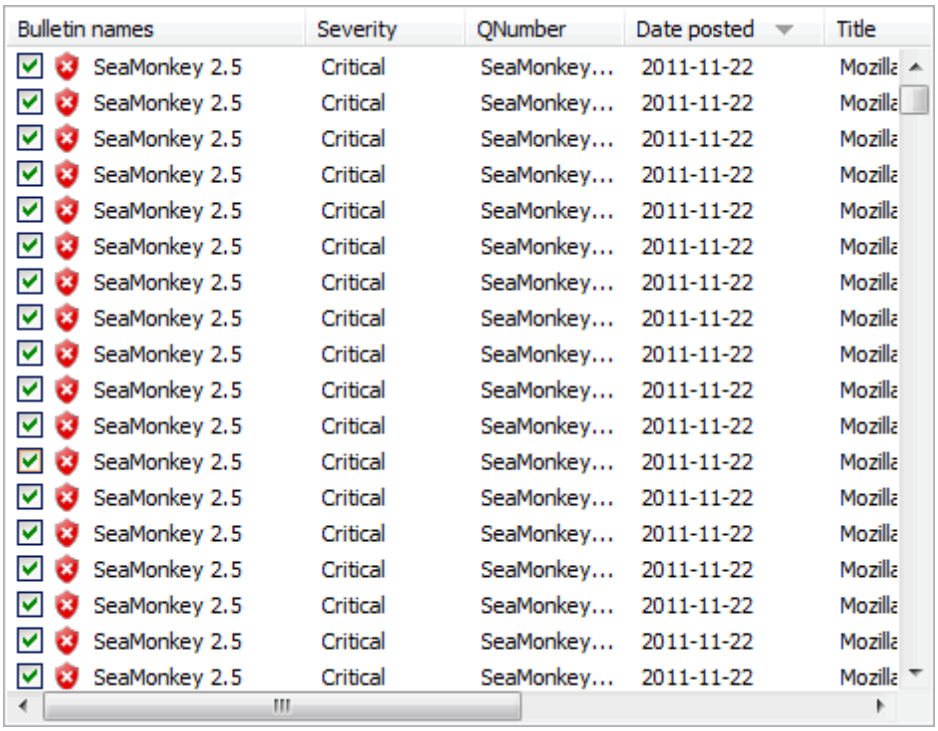
> **Note**
>
> Missing patch scanning parameters are configurable on a scan profile by scan profile basis. Make sure to enable missing patch scanning in all profiles where missing patch scanning is required.

12.3.2 Customizing the list of software patches to scan

To specify which missing security updates will be enumerated and processed by a scanning profile:

1. From the **Vulnerability Assessment Options** tab, click **Patches** sub-tab

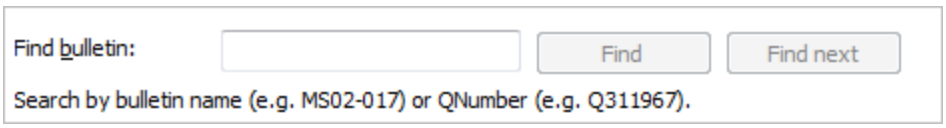
2. Select the scanning profile to customize from the left pane under **Profiles**.



Screenshot 139: Select the missing patches to enumerate

3. In the right pane, select/unselect which missing patches are enumerated by this scanning profile.

12.3.3 Searching for Bulletin Information

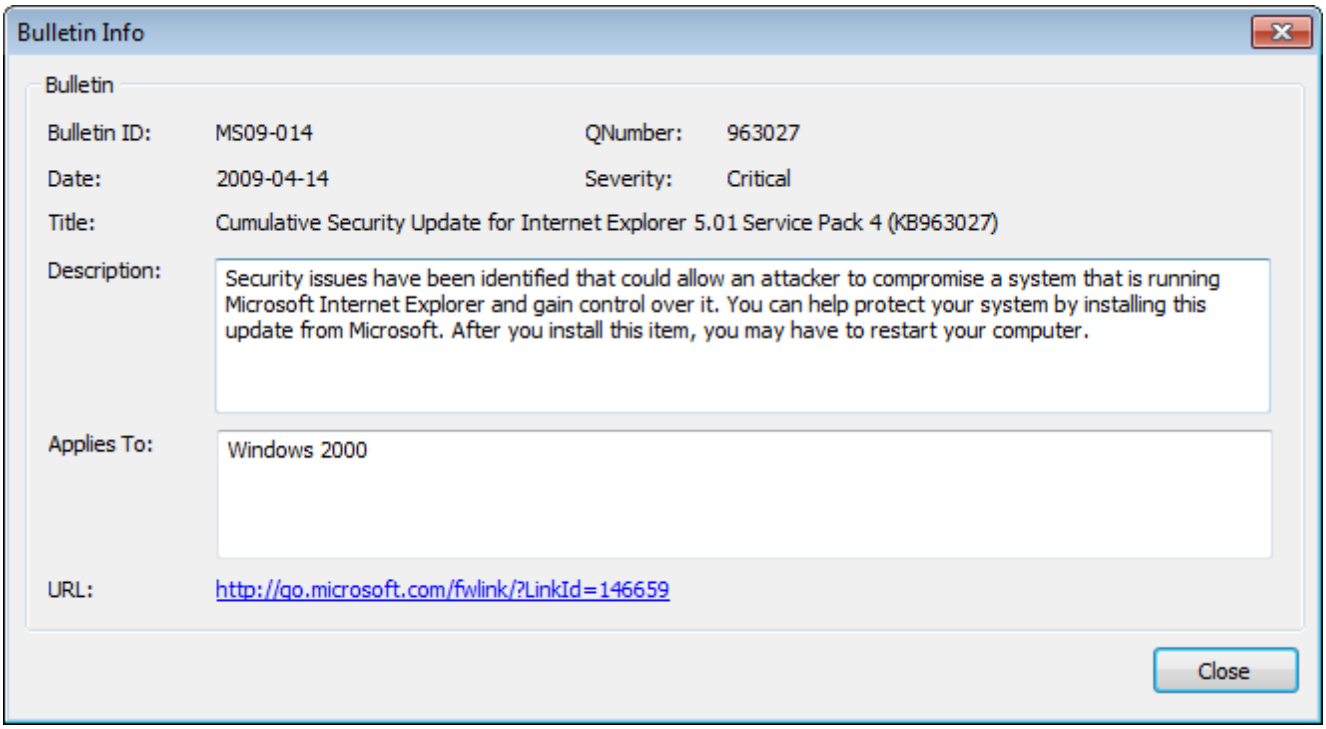


Screenshot 140: Searching for bulletin information

To search for a particular bulletin:

1. From **Vulnerability Assessment Options > Vulnerabilities > Find bulletin**, specify the bulletin name (example: MS02-017) or QNumber (example: Q311987), in the search tool entry box included at the bottom of the right pane.

2. Click **Find** to search for your entry.


Bulletin Info
Bulletin
Bulletin ID:
MS09-014
QNumber:
963027
Date:
2009-04-14
Severity:
Critical
Title:
Cumulative Security Update for Internet Explorer 5.01 Service Pack 4 (KB963027)
Description:
Security issues have been identified that could allow an attacker to compromise a system that is running Microsoft Internet Explorer and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this item, you may have to restart your computer.
Applies To:
Windows 2000
URL:
http://go.microsoft.com/fwlink/?LinkId=146659
Close

Screenshot 141: Extended bulletin information

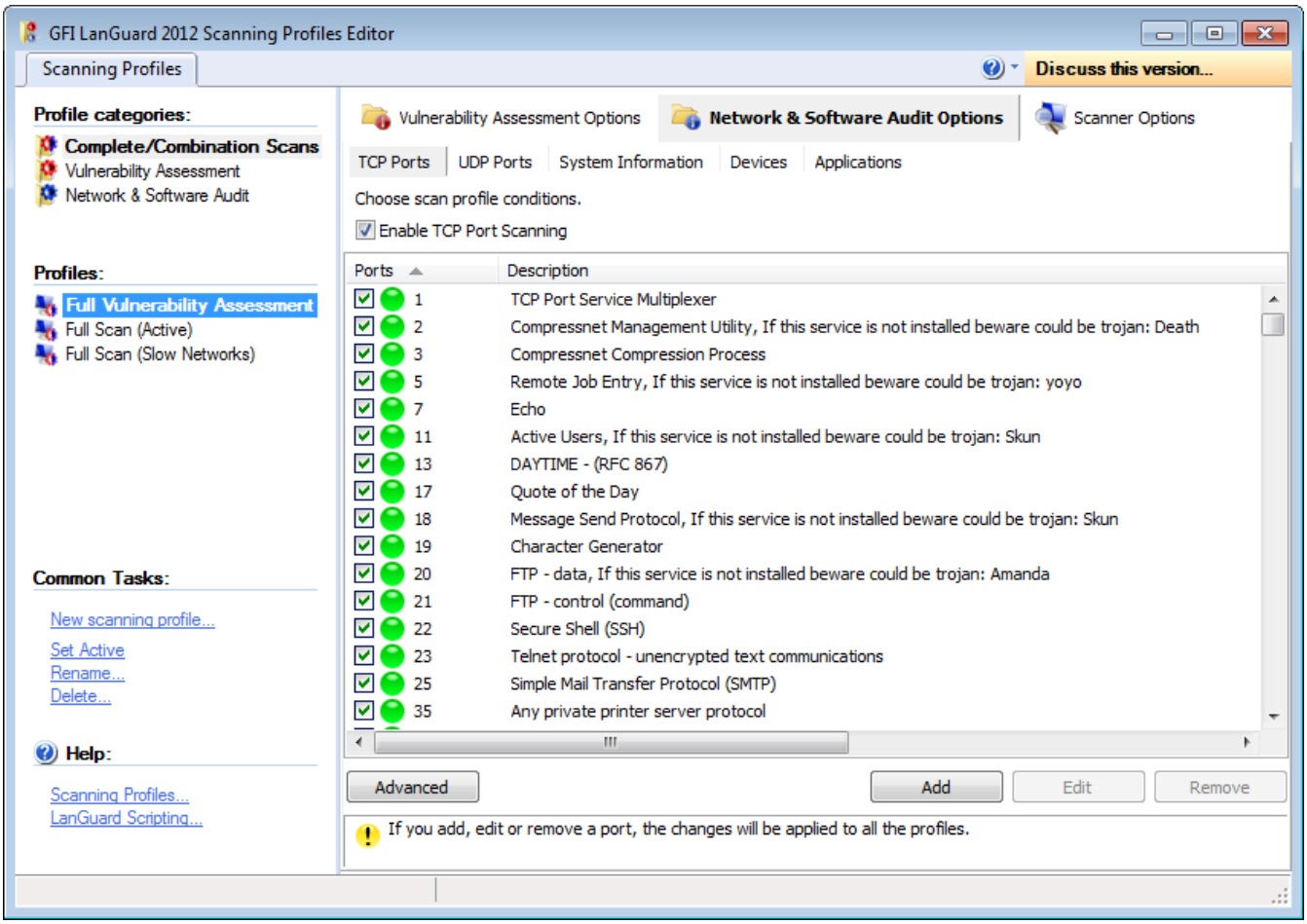
12.4 Configuring Network & Software Audit options

The scanning profiles that ship with GFI LanGuard are already pre-configured to run a number of network and software audit checks on selected target. You can however disable scanning as well as customize the list of network and software audits executed during a scan.

This section contains information about:

- Configuring TCP/UDP port scanning options
- Configuring System Information options
- Configuring Device scanning options
- Configuring Applications scanning options

12.4.1 Configuring TCP/UDP port scanning options


GFI LanGuard 2012 Scanning Profiles Editor
Scanning Profiles
Discuss this version...
Profile categories:
Complete/Combination Scans
Vulnerability Assessment
Network & Software Audit
Profiles:
Full Vulnerability Assessment
Full Scan (Active)
Full Scan (Slow Networks)
Common Tasks:
New scanning profile...
Set Active
Rename...
Delete...
Help:
Scanning Profiles...
LanGuard Scripting...
Vulnerability Assessment Options
Network & Software Audit Options
Scanner Options
TCP Ports
UDP Ports
System Information
Devices
Applications
Choose scan profile conditions.
Enable TCP Port Scanning
Ports
Description
1 TCP Port Service Multiplexer
2 Compressnet Management Utility, If this service is not installed beware could be trojan: Death
3 Compressnet Compression Process
5 Remote Job Entry, If this service is not installed beware could be trojan: yoyo
7 Echo
11 Active Users, If this service is not installed beware could be trojan: Skun
13 DAYTIME - (RFC 867)
17 Quote of the Day
18 Message Send Protocol, If this service is not installed beware could be trojan: Skun
19 Character Generator
20 FTP - data, If this service is not installed beware could be trojan: Amanda
21 FTP - control (command)
22 Secure Shell (SSH)
23 Telnet protocol - unencrypted text communications
25 Simple Mail Transfer Protocol (SMTP)
35 Any private printer server protocol
Advanced
Add
Edit
Remove
If you add, edit or remove a port, the changes will be applied to all the profiles.

Screenshot 142: Scanning Profiles properties: TCP Ports tab options

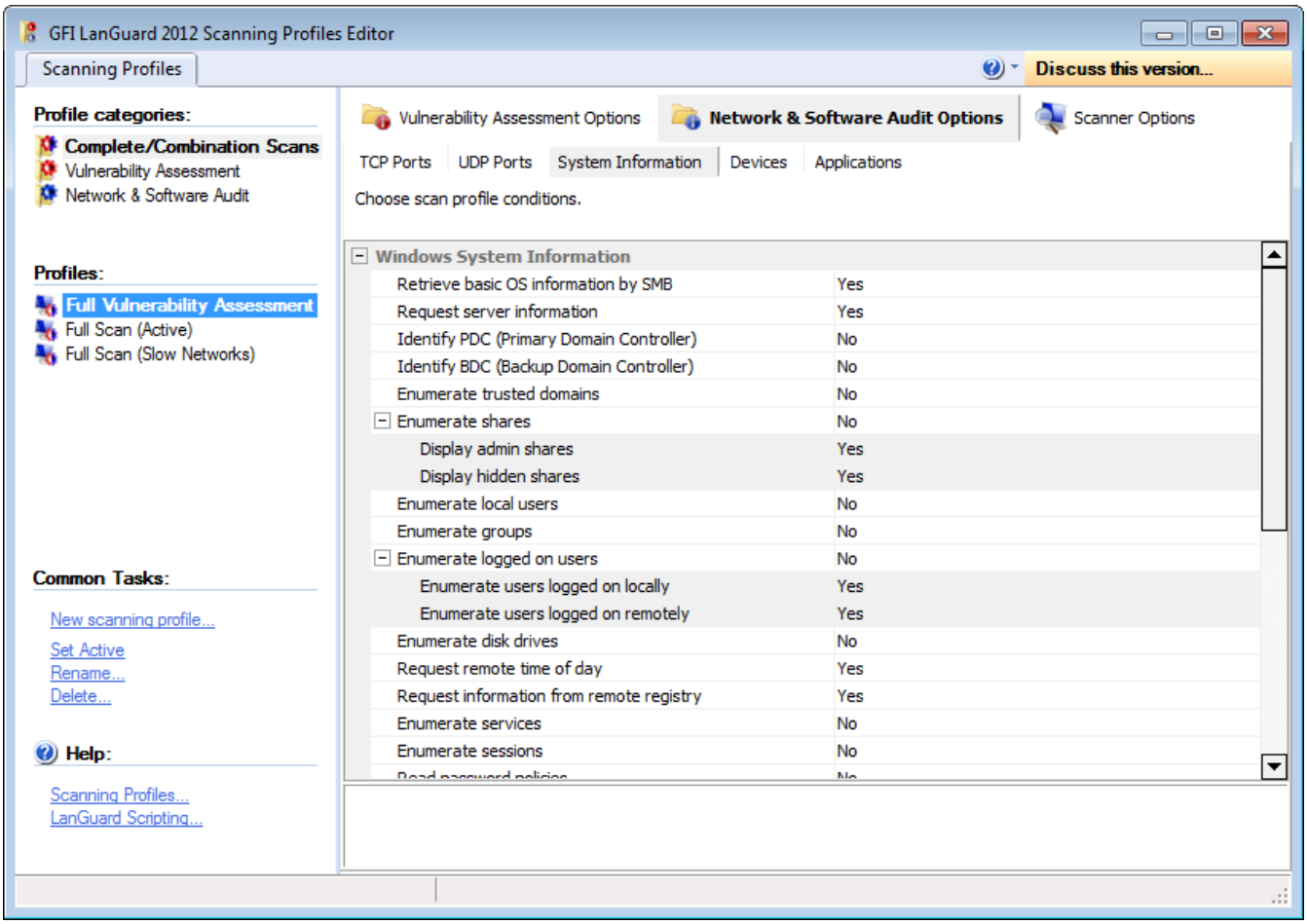
Table 78: TCP Port scanning options

Option	Description
Enabling/disabling TCP Port scanning	To enable TCP Port Scanning in a particular scanning profile: 1. From the **Network & Security Audit Options** tab, click **TCP Ports** sub-tab. 2. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 3. Select **Enable TCP Port Scanning** option.
Configuring the list of TCP ports to be scanned	To configure which TCP ports will be processed by a scanning profile: 1. From **Network & Security Audit Options** tab, click **TCP Ports** sub-tab. 2. Select scanning profile to customize from the left pane under **Profiles**. 3. Select TCP ports to analyze with this scanning profile.
Customizing the list TCP ports	1. From the **Network & Security Audit Options** tab, click **TCP Ports** sub-tab. 2. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 3. Customize the list of TCP Ports through **Add**, **Edit** or **Remove**.

Note

The list of supported TCP/UDP Ports is common for all profiles. Deleting a port from the list will make it unavailable for all scanning profiles

12.4.2 Configuring System Information options



Screenshot 143: Scanning Profiles properties: System Information tab options

To specify what **System Information** is enumerated by a particular scanning profile:

1. From the **Network & Security Audit Options** tab, click **System Information** sub-tab.

2. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

3. From the right pane, expand the **Windows System Information** group or Linux System Information group accordingly.

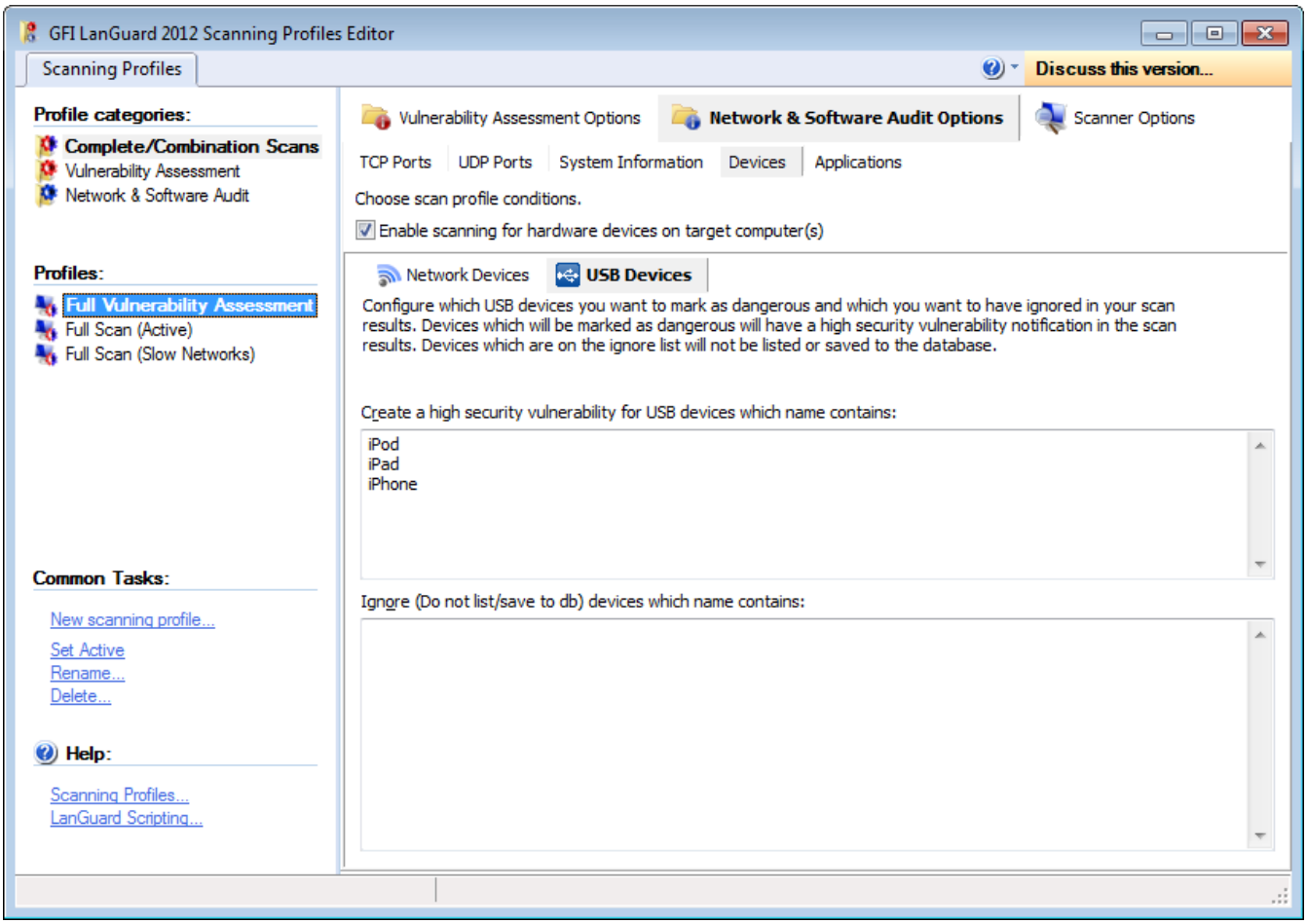
4. Select which Windows/Linux OS information is retrieved by the security scanner from scanned targets.

For example, to enumerate administrative shares in scan results, expand the **Enumerate shares** option and set the **Display admin shares** option to '**Yes**'.

12.4.3 Configuring Device scanning options

Use the Devices tab to enumerate network devices. Together with device enumeration, you can further configure GFI LanGuard to generate high security vulnerability alerts whenever a USB or Network device is detected.

This is achieved by compiling a list of unauthorized/blacklisted Network and USB devices that you want to be alerted.


GFI LanGuard 2012 Scanning Profiles Editor
Scanning Profiles
Discuss this version...
Profile categories:
Complete/Combination Scans
Vulnerability Assessment
Network & Software Audit
Profiles:
Full Vulnerability Assessment
Full Scan (Active)
Full Scan (Slow Networks)
Common Tasks:
New scanning profile...
Set Active
Rename...
Delete...
Help:
Scanning Profiles...
LanGuard Scripting...
Vulnerability Assessment Options
Network & Software Audit Options
Scanner Options
TCP Ports
UDP Ports
System Information
Devices
Applications
Choose scan profile conditions.
Enable scanning for hardware devices on target computer(s)
Network Devices
USB Devices
Configure which USB devices you want to mark as dangerous and which you want to have ignored in your scan results. Devices which will be marked as dangerous will have a high security vulnerability notification in the scan results. Devices which are on the ignore list will not be listed or saved to the database.
Create a high security vulnerability for USB devices which name contains:
iPod
iPad
iPhone
Ignore (Do not list/save to db) devices which name contains:

Screenshot 144: The network devices configuration page

GFI LanGuard can also exclude from the scanning process specific USB devices that you consider safe. Such devices can be a USB mouse or keyboard. This is achieved through a safe/white list of USB devices to ignored during scanning.

Similarly you can create a separate scanning profile that enumerates only Bluetooth dongles and wireless NIC cards connected to your target computers. In this case however, you must specify 'Bluetooth' and 'Wireless' or 'WiFi' in the unauthorized network and USB lists of your scanning profile.

All the device scanning configuration options are accessible through the two sub-tabs contained in the devices configuration page. These are the **Network Devices** tab and the **USB Devices** tab.

Use the **Network Devices** sub-tab to configure the attached network devices scanning options and blacklisted (unauthorized)/white-listed (safe) devices lists.

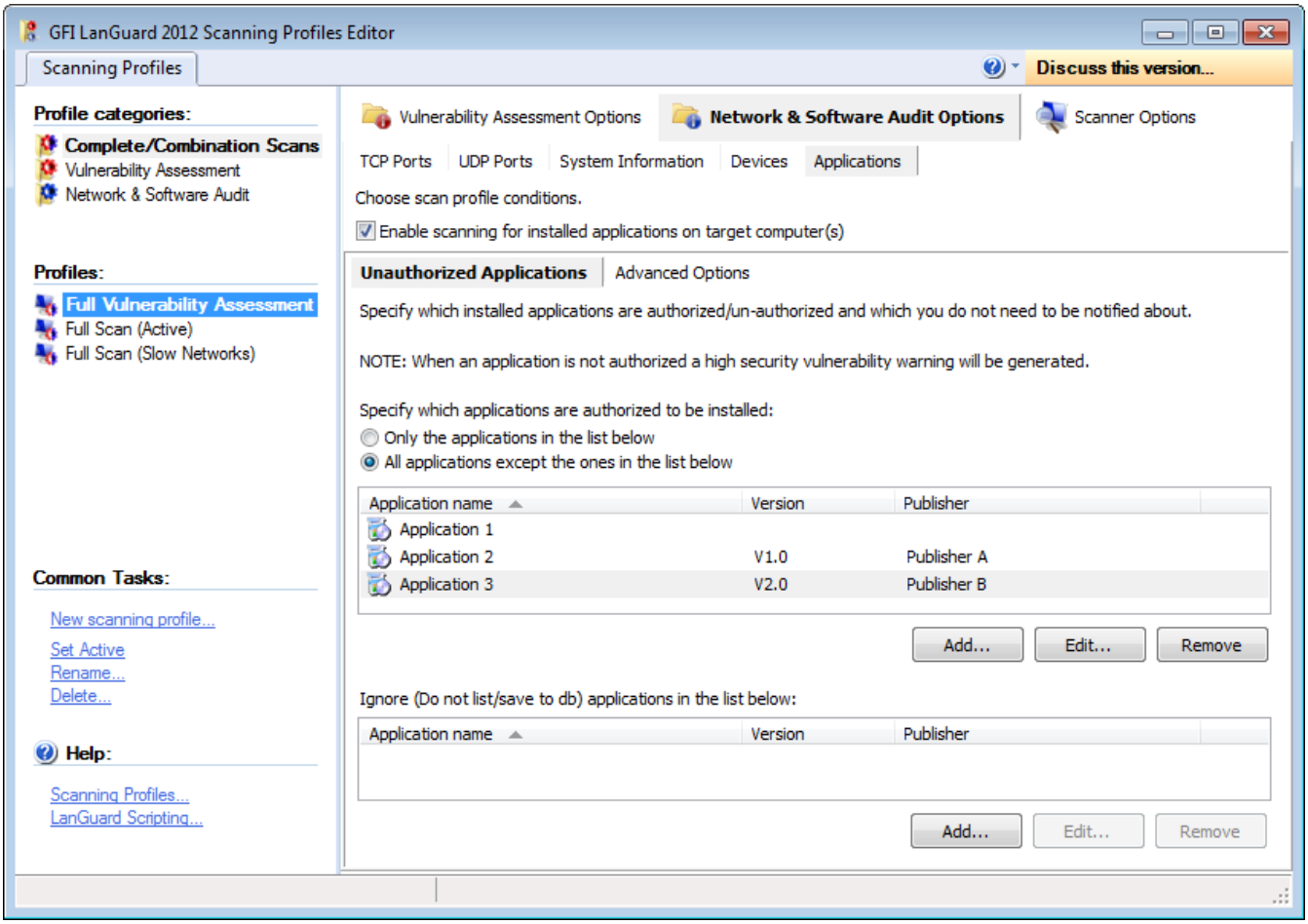
Use the **USB Devices** sub-tab to configure the attached USB devices scanning options and unauthorized/safe devices lists.

Table 79: Device scanning options

Option	Description
Enabling/disabling checks for all installed network devices	To enable network device (including USB device) scanning in a particular scanning profile: 1. From the **Network & Security Audit Options** tab, click **Devices** sub-tab. 2. Click **Network Devices** tab. 3. Select the scanning profile to customize from the left pane under **Profiles**. 4. From the right pane, select **Enable scanning for hardware devices** on target computer(s). **Note** Network device scanning is configurable on a scan profile by scan profile basis. Make sure to enable network device scanning in all profiles where this is required.
Compiling a network device black-list/white-list	To compile a network device blacklist/white-list for a scanning profile: 1. From the **Network & Security Audit Options** tab, click **Devices** sub-tab. 2. Click **Network Devices** tab. 3. Select the scanning profile to customize from the left pane under **Profiles**. 4. In the right pane: to create a network device blacklist, specify which devices you want to classify as high security vulnerabilities in the space provided under **Create a high security vulnerability for network devices which name contains**. For example, if you enter the word 'wireless' you will be notified through a high security vulnerability alert when a device whose name contains the word 'wireless' is detected. To create a network device white-list, specify which devices you want to ignore during network vulnerability scanning in the space provided under **Ignore (Do not list/save to db)** devices which name contains. **Note** Only include one network device name per line.
Configuring advanced network device scanning options	From the **Network Devices** tab, you can also specify the type of network devices checked by this scanning profile and reported in the scan results. These include 'wired network devices', 'wireless network devices', 'software enumerated network devices' and 'virtual network devices'. To specify which network devices to enumerate in the scan results: 1. From the **Network & Security Audit Options** tab, click **Devices** sub-tab. 2. Click on the **Network Devices** tab (opens by default). 3. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 4. Click **Advanced** at the bottom of the page. 5. Set the required options to **Yes**. Click **OK** to finalize your settings.
Scanning for USB devices	To compile a list of unauthorized/unsafe USB devices: 1. From the **Network & Security Audit Options** tab, click the **Devices** sub-tab. 2. Click **USB Devices** tab. 3. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 4. In the right pane. specify which devices you want to classify as high security vulnerabilities in the space provided under **Create high security vulnerability for USB devices which name contains:**. For example, if you enter the word 'iPod', you will be notified through a high security vulnerability alert when a USB device whose name contains the word 'iPod' is detected. To create a USB device white-list, specify which USB devices you want to ignore during network vulnerability scanning in the space provided under **Ignore (Do not list/save to db) devices which name contains**. **Note** Only include one USB device name per line.

12.4.4 Configuring Applications scanning options

The **Applications** tab enables you to specify which applications will trigger an alert during a scan.



Screenshot 145: The applications configuration page

Through this tab, you can also configure GFI LanGuard to detect and report unauthorized software installed on scanned targets and to generate high security vulnerability alerts whenever such software is detected.

Table 80: Applications scanning options

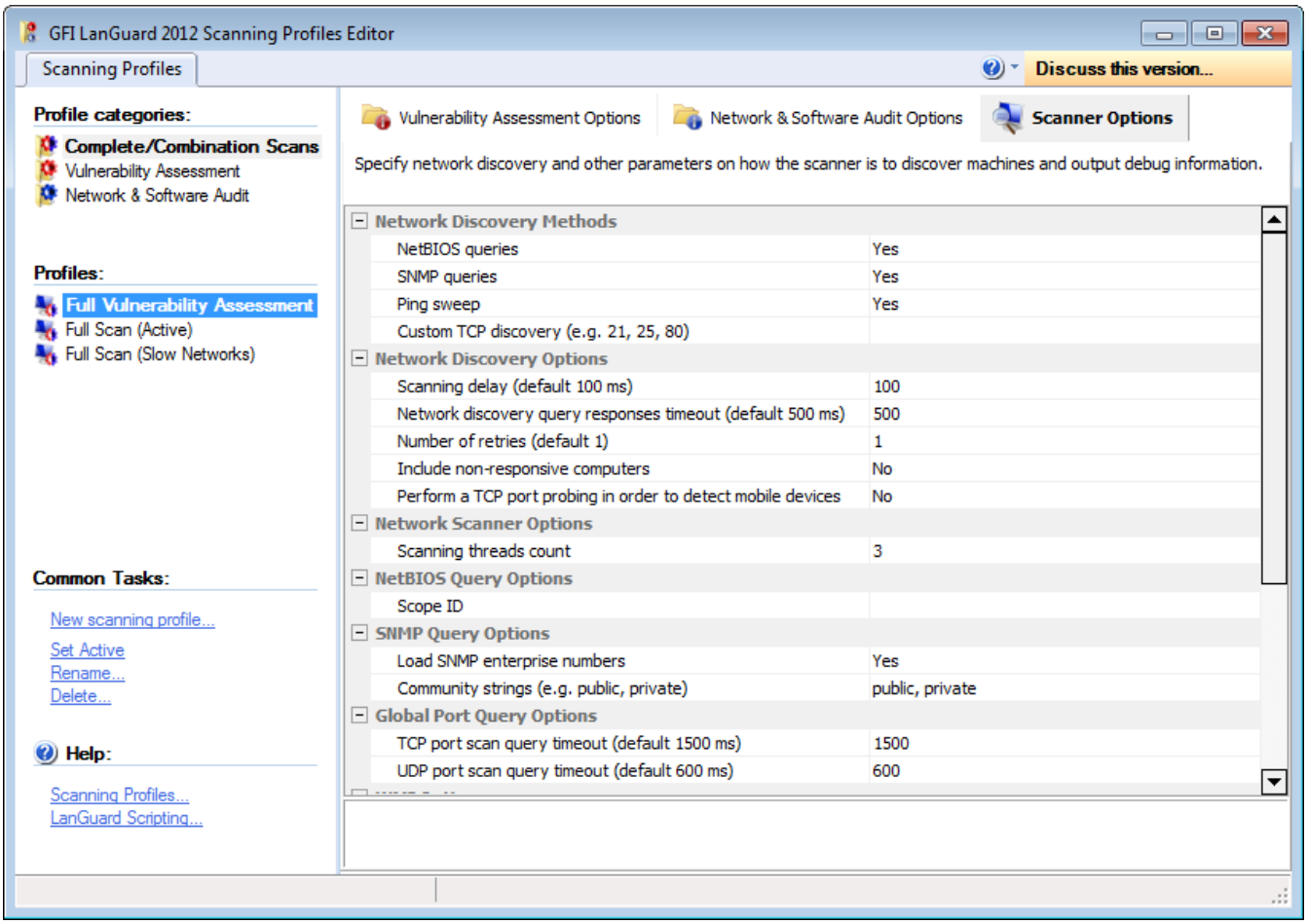
Option	Description
Scanning installed applications	By default,GFI LanGuard also supports integration with particular security applications. These include various anti-virus and anti-spyware software. During security scanning, GFI LanGuard checks the correct configuration of virus scanner(s) or anti-spyware software and that the respective definition files are up to date. Application scanning is configurable on a scan profile by scan profile basis and all the configuration options are accessible through the two sub-tabs contained in the **Applications** tab. These are the **Unauthorized Applications** sub-tab and the **Advanced Options** sub-tab.
Enabling/disabling checks for installed applications	To enable installed applications scanning in a particular scanning profile: 1. From the **Network & Security Audit Options** tab, click on the **Applications** sub-tab. 2. Click on the **Unauthorized Applications** sub-tab. 3. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 4. Select the **Enable scanning for installed applications on target computer(s)** checkbox. **Note** Installed applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable installed applications scanning in all profiles where this is required.

Option	Description
Compiling installed applications black-list/white-list	To compile installed applications blacklist/white-list: 1. From the **Network & Security Audit Options** tab, click **Applications** sub-tab. 2. Select **Unauthorized Applications** sub-tab. 3. Select the scanning profile to customize from the left pane under **Profiles**. 4. From the right pane, select **Enable scanning for installed applications on target computer(s)** checkbox. 5. Specify the applications that are authorized for installation. Select from: » **Only the applications in the list below** - Specify names of applications that are authorized for installation. These applications will be ignored during a security scan » **All applications except the ones in the list below** - Specify the names of the applications that are unauthorized for installation. Applications not in this list will be ignored during a security scan. 6. In the **Ignore (Do not list/save to db) applications from the list below** options key in applications by clicking **Add**. Any application listed is white-listed. **Note** Include only one application name per line.
Advanced application scanning options	GFI LanGuard ships with a default list of anti-virus and anti-spyware applications that can be checked during security scanning. The **Advanced Options** tab enables you to configure when GFI LanGuard will generate high security vulnerability alerts if it detects certain configurations of a security application. Alerts are generated when: » No anti-virus, anti-spyware or firewall is detected » A fake anti-virus or anti-spyware is detected » Anti-virus or anti-spyware definitions are not up to date » Anti-virus or anti-spyware real-time monitoring is turned off » Anti-virus or anti-spyware product is expired » Anti-virus or anti-spyware product detects malware on the scanned computer(s) » Firewall is disabled » HTTP/FTP timeout when checking for product updates on remote sites. This option generates an alert if the number of seconds defined for timeout is exceeded.

Option	Description
Enabling/disabling checks for security applications	To enable checks for installed security applications in a particular scanning profile: 1. From the **Network & Security Audit Options** tab, click on the **Applications** sub-tab. 2. Click on the **Advanced Options** tab. 3. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 4. Select **Enable scanning for installed applications on target computer(s)** checkbox. 5. (Agent-less scans) Select **Enable full security applications audit for agent-less scans** checkbox. **Note** 1. Agent-less scans temporarily runs a small service on the remote computers in order to retrieve the relevant information. 2. Security applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable security applications scanning in all profiles where this is required. 3. The number of supported security applications is constantly updated. Click the link available in order to get the latest version of the list. Configuring security applications - advanced options. To configure alerting triggers for installed security applications in a particular scanning profile: 1. From **Network & Security Audit Options** tab, click **Applications** sub-tab. 2. Click **Advanced Options** tab. 3. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 4. Select **Enable scanning for installed applications on target computer(s)** checkbox. 5. (Agent-less scans) Select **Enable full security applications audit for agent-less scans** checkbox. 6. From the bottom-right pane, select the trigger you want to configure and choose between **Yes or** No from the drop down menu next to the respective alert trigger. **Note** Security applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable security applications scanning in all profiles where this is required.

12.5 Configuring security scanning options

Use **Scanner Options** tab to configure the operational parameters of the security-scanning engine. These parameters are configurable on a scan profile by scan profile basis and define how the scanning engine will perform target discovery and OS Data querying.


GFI LanGuard 2012 Scanning Profiles Editor
Scanning Profiles
Discuss this version...
Profile categories:
Complete/Combination Scans
Vulnerability Assessment
Network & Software Audit
Profiles:
Full Vulnerability Assessment
Full Scan (Active)
Full Scan (Slow Networks)
Common Tasks:
New scanning profile...
Set Active
Rename...
Delete...
Help:
Scanning Profiles...
LanGuard Scripting...
Vulnerability Assessment Options
Network & Software Audit Options
Scanner Options
Specify network discovery and other parameters on how the scanner is to discover machines and output debug information.
Network Discovery Methods
NetBIOS queries Yes
SNMP queries Yes
Ping sweep Yes
Custom TCP discovery (e.g. 21, 25, 80)
Network Discovery Options
Scanning delay (default 100 ms) 100
Network discovery query responses timeout (default 500 ms) 500
Number of retries (default 1) 1
Include non-responsive computers No
Perform a TCP port probing in order to detect mobile devices No
Network Scanner Options
Scanning threads count 3
NetBIOS Query Options
Scope ID
SNMP Query Options
Load SNMP enterprise numbers Yes
Community strings (e.g. public, private) public, private
Global Port Query Options
TCP port scan query timeout (default 1500 ms) 1500
UDP port scan query timeout (default 600 ms) 600

Screenshot 146: Scanning Profiles properties: Scanner Options tab

Configurable options include timeouts, types of queries to run during target discovery, number of scanning threads count, SNMP scopes for queries and more.

> **Important**
>
> Configure these parameters with extreme care! An incorrect configuration can affect the security scanning performance of GFI LanGuard.

To configure scanner options:

1. From **Scanning Profile Editor > Profile categories**, select the category that contains the scanning profile you want to edit (example: **Complete/Combination Scans**).

2. From the **Profiles** section, select the scanning profile you want to edit (example: **Full Vulnerability Assessment**).

3. From the right pane, click **Scanner Options**.

4. Configure the following parameters that determine the scanning behavior of GFI LanGuard:

Table 81: Scanner Options

Parameter	Description
Network Discovery Methods	
NetBIOS queries	Enable/disable the use of NetBios queries to discover network devices.
SNMP queries	Enable/disable the use of SNMP queries to discover network devices.

Parameter	Description
Ping sweep	Enable/disable the use of Ping sweeps to discover network devices.
Custom TCP discovery	Discover online machines by querying for the specified open TCP ports.
Network Discovery Options	
Scanning delay	Key in the time interval (in milliseconds) between one scan and another.
Network discovery query responses timeout	Amount of time in milliseconds the security scanner will wait before timing out when performing a machine discovery query (NetBIOS/SNMP/Ping).
Number of retries	Number of times security scanner will retry to connect to a non-responsive machine before skipping it.
Include non-responsive computers	Run scans on all the PCs regardless of whether they are detected as being online or not.
Perform a TCP port probing in order to detect mobile devices	Perform a TCP port probing in order to detect mobile devices using known ports.
Network Scanner Options	
Scanning threads count	Key in the number of scan threads that can run simultaneously.
NetBIOS Query Options	
Scope ID	Used for NetBIOS environments requiring a specific scope ID in order to allow querying.
SNMP Query Options	
Load SNMP enterprise numbers	Specifies whether security scanner should use the OID (Object Identifier database) containing ID to Vendor map to identify the various types of devices.
Community strings	Specifies whether security scanner should use the specified community string for SNMP server detection and information retrieval.
Global Port Query Options	
TCP port scan query timeout	Amount of time in milliseconds security scanner will wait during a TCP port scan before timing out and moving on to scan the next port.
UDP port scan query timeout	Amount of time in milliseconds security scanner will wait during a UDP port scan before timing out and moving on to scan the next port.
WMI Options	
WMI timeout	Amount of time in milliseconds security scanner will wait for a reply from the remote WMI server before timing out and moving on to the next scan item.
SSH Options	
SSH timeout	Amount of time in milliseconds security scanner will wait for a SSH script to return before timing out and moving on to the next scan item.
Alternative SSH port	Alternative SSH ports to use when the default port 22 is unreachable.
Scanner activity window	
Type of scanner activity output	Activity progress modes: simple (basic progress - start / stop of operations), or verbose (more detailed information on process flow).
Display received packets	Output TCP packets in raw format as they were received by security scanner.
Display sent packets	Output TCP packets in raw format as they were sent by security scanner.
OS Information Retrieval Options	
Create custom share if administrative privileges are disabled	If administrative shares are disabled the scanner will temporarily create a custom hidden share of the form <random GUID>$. The share is used to retrieve data that helps identifying vulnerabilities and missing patches.
Start remote registry	If the remote registry service is stopped on the scanned machine, enable this option to temporarily open it during the security scanning.

13 Utilities

GFI LanGuard provides you with a set of network utilities that enable you to monitor network activity, gather network information and audit network devices.

Topics in this chapter:

13.1 DNS Lookup 212

13.2 Traceroute 215

13.3 Whois 216

13.4 Enumerate Computers 217

13.5 Enumerate Users 219

13.6 SNMP Auditing 220

13.7 SNMP Walk 221

13.8 SQL Server® Audit 222

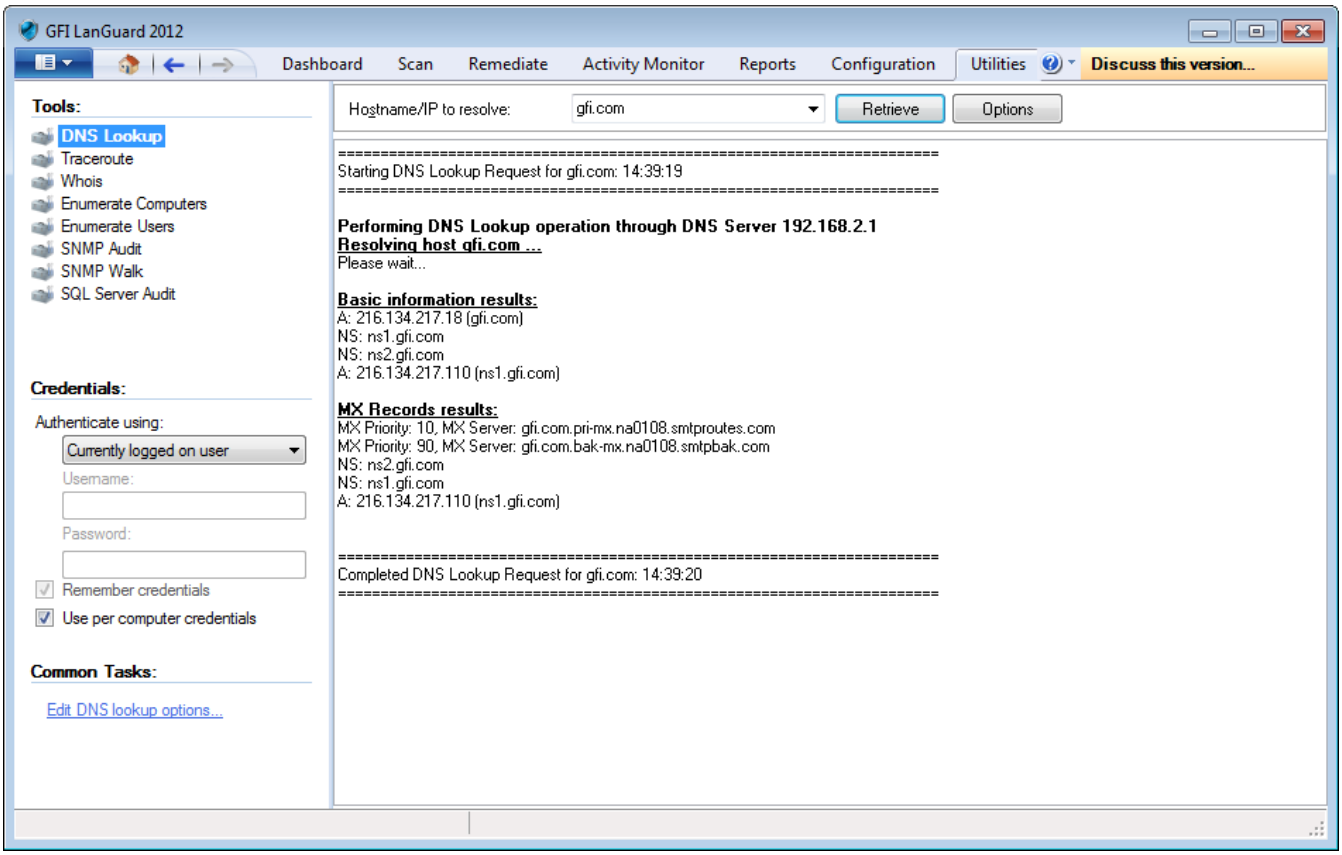
13.9 Command Line Tools 223

13.1 DNS Lookup

DNS lookup resolves domain names into the corresponding IP address and retrieves particular information from the target domain (for example, MX record, etc.).

To resolve a domain/host name:

1. Launch GFI LanGuard.
2. Click **Utilities** tab and select **DNS Lookup** in the left pane under **Tools**.
3. Specify the hostname to resolve in **Hostname/IP to resolve**.



Screenshot 147: DNS Lookup tool

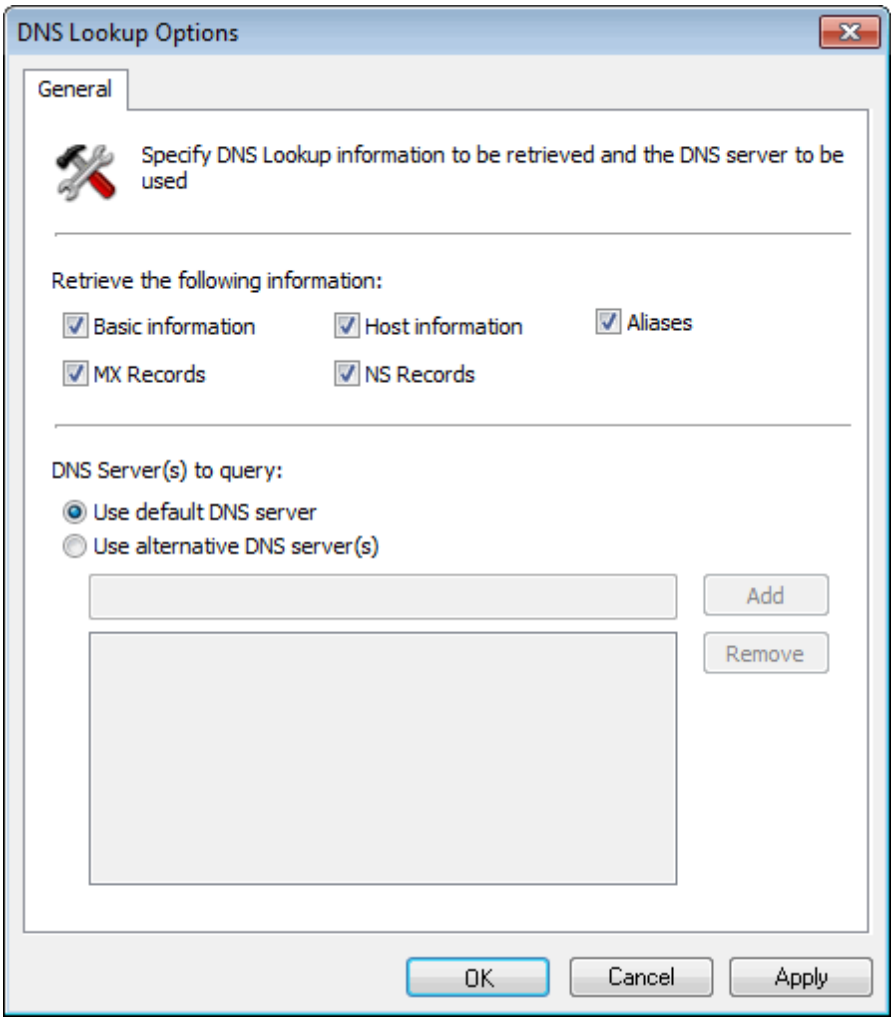
4. Under **Common Tasks** in the left pane, click on **Edit DNS Lookup options** or click **Options** on the right pane and specify the information described below:

Table 82: DNS lookup options

Option	Description
Basic Information	Retrieve the host name and the relative IP address.
Host Information	Retrieve HINFO details. The host information (known as HINFO) generally includes target computer information such as hardware specifications and OS details.
Aliases	Retrieve information on the 'A Records' configured on the target domain.
MX Records	Enumerate all the mail servers and the order (i.e. priority) in which they receive and process emails for the target domain.
NS Records	Specify the 'name-servers' that are authoritative for a particular domain or sub domain.

Note

Some DNS entries do not contain certain information for security reasons.



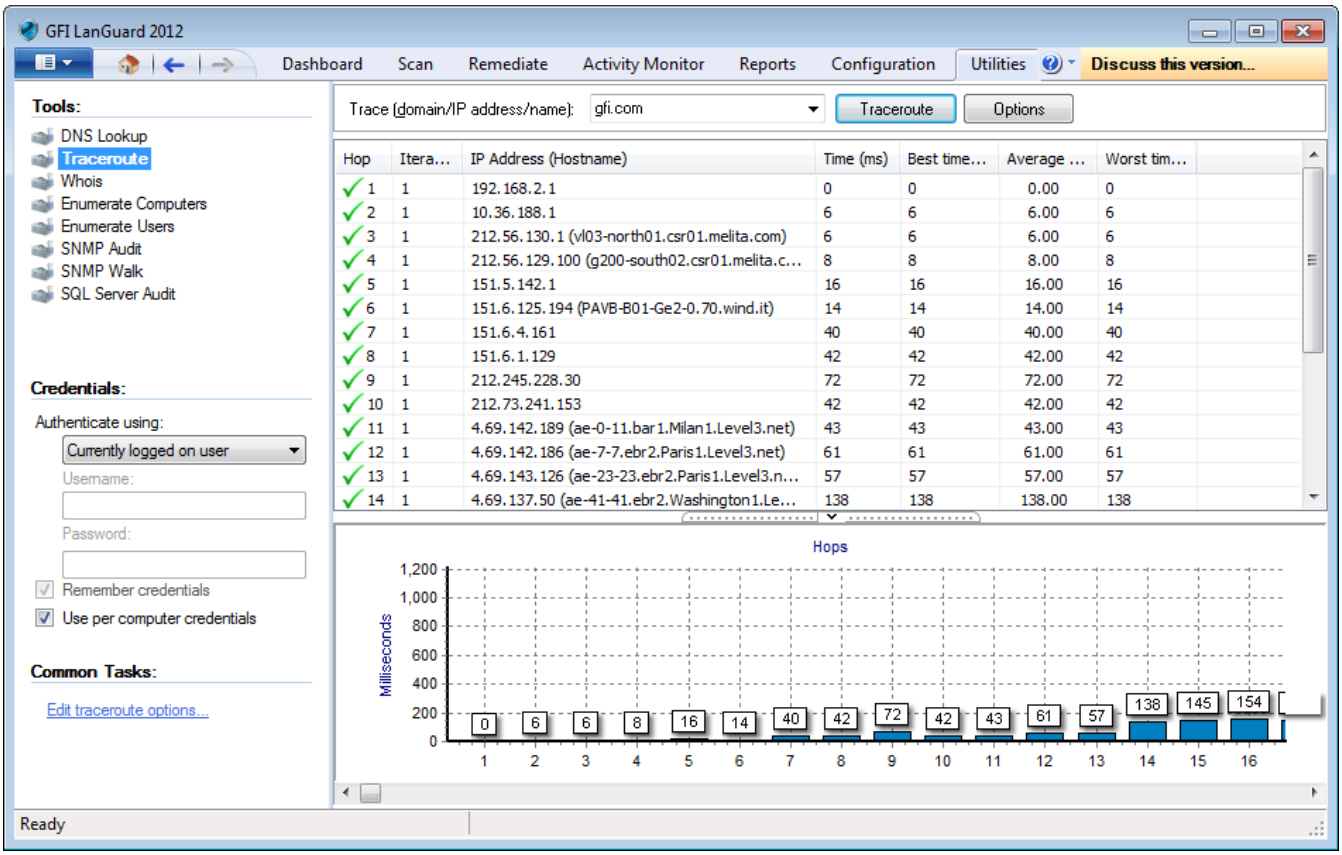
Screenshot 148: DNS Lookup tool options

5. (Optional) Specify the alternative DNS server that will be queried by the DNS Lookup tool or leave as default to use the default DNS server.

6. Click **Retrieve** to start the process.

13.2 Traceroute

Traceroute identifies the path that GFI LanGuard followed to reach a target computer.



Screenshot 149: Traceroute tool

To use the Traceroute tool:

1. Launch GFI LanGuard.

2. Click **Utilities** tab and select **Traceroute** in the left pane under **Tools**.

3. In the **Trace (domain/IP/name)**, specify the name/IP or domain to reach.

4. (Optional) Under **Common Tasks** in the left pane, click on **Edit Traceroute options** or click **Options** on the right pane to change the default options.

5. Click on the **Traceroute** button to start the tracing process.

Traceroute will break down, the path taken to a target computer into 'hops'. A hop indicates a stage and represents a computer that was traversed during the process.

The information enumerated by this tool includes the IP of traversed computers, the number of times that a computer was traversed and the time taken to reach the respective computer. An icon is also included next to each hop. This icon indicates the state of that particular hop. The icons used in this tool include:

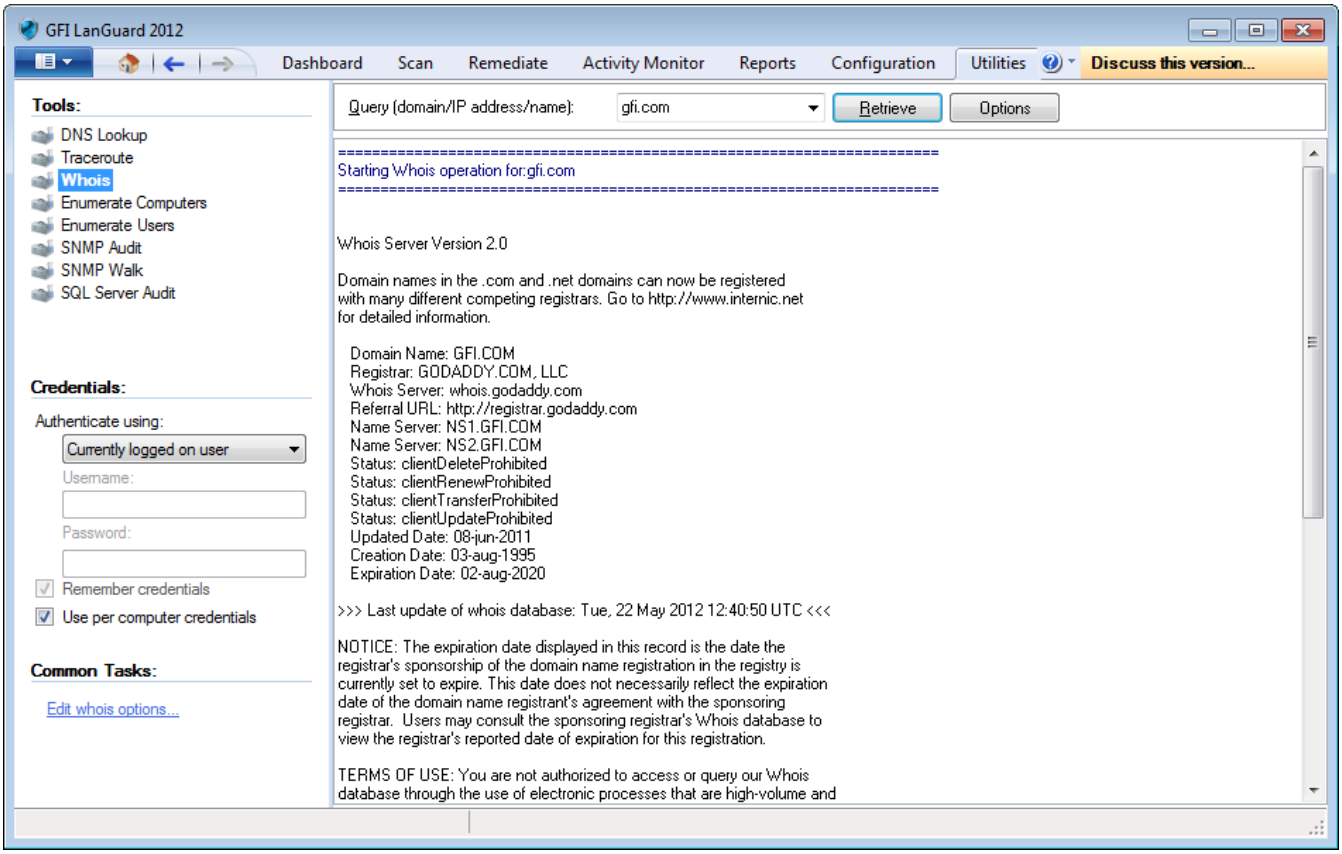
Table 83: Traceroute icons

Icon	Description
	Indicates a successful hop taken within normal parameters.
	Indicates a successful hop, but time required was quite long.

Icon	Description
	Indicates a successful hop, but the time required was too long.
	Indicates that the hop was timed out (> 1000ms).

13.3 Whois

Whois looks up information on a particular domain or IP address.



Screenshot 150: Whois tool

1. Launch GFI LanGuard.

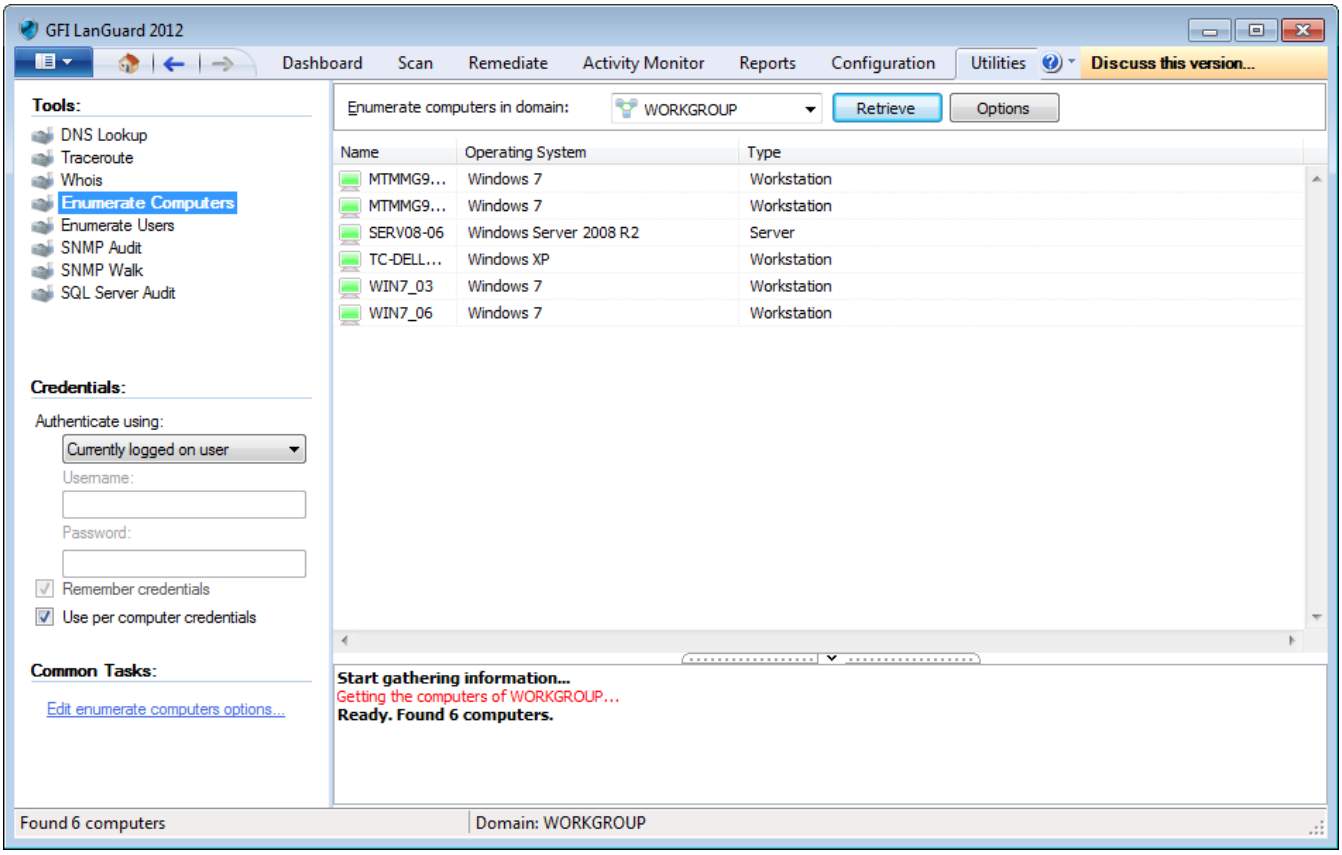
2. Click **Utilities** tab and select **Whois** in the left pane under **Tools**.

3. In **Query (domain/IP/name)** menu, specify the name/IP or domain to reach.

4. (Optional) From **Common Tasks** in the left pane, click **Edit Whois options** or **Options** on the right pane to change the default options.

5. Click **Retrieve** to start the process.

13.4 Enumerate Computers



Screenshot 151: Enumerate Computers tool

The enumerate computers utility identifies domains and workgroups on a network. During execution, this tool will also scan each domain/workgroup discovered so to enumerate their respective computers.

- The information enumerated by this tool includes:
- The domain or workgroup name
- The list of domain/workgroup computers
- The operating system installed on the discovered computers
- Any additional details that might be collected through NetBIOS.

Computers are enumerated using one of the following methods:

Table 84: Enumerate computers options

Option	Description
From Active Directory®	This method is much faster and will include computers that are currently switched off.
From Windows Explorer	This method enumerates computers through a real-time network scan and therefore it is slower and will not include computers that are switched off.

To enumerate computers:

1. Launch GFI LanGuard.
2. Click **Utilities** tab and select **Enumerate Computers** in the left pane under **Tools**.
3. In the **Enumerate computers in domain**, select the desired domain.

4. From **Common Tasks** in the left pane, click **Edit Enumerate Computers options** or **Options** on the right pane.

5. Select whether to enumerate computers from Active Directory® or Windows Explorer.

6. Click **Retrieve** to start the process.

> **Note**
>
> For an Active Directory® scan, you will need to run the tool under an account that has access rights to Active Directory®.

13.4.1 Starting a Security Scan

To start a security scan directly from the 'Enumerate Computers' tool, right-click on any of the enumerated computers and select Scan.

You can also launch a security scan and at the same time continue using the Enumerate Computers tool. This is achieved by right-clicking on any of the enumerated computers and selecting Scan in background.

13.4.2 Deploying Custom Patches

You can use the Enumerate Computers tool to deploy custom patches and third party software on the enumerated computers. To launch a deployment process directly from this tool:

1. Select the computers that require deployment.

2. Right-click on any of the selected computers and select **Deploy Custom Patches**.

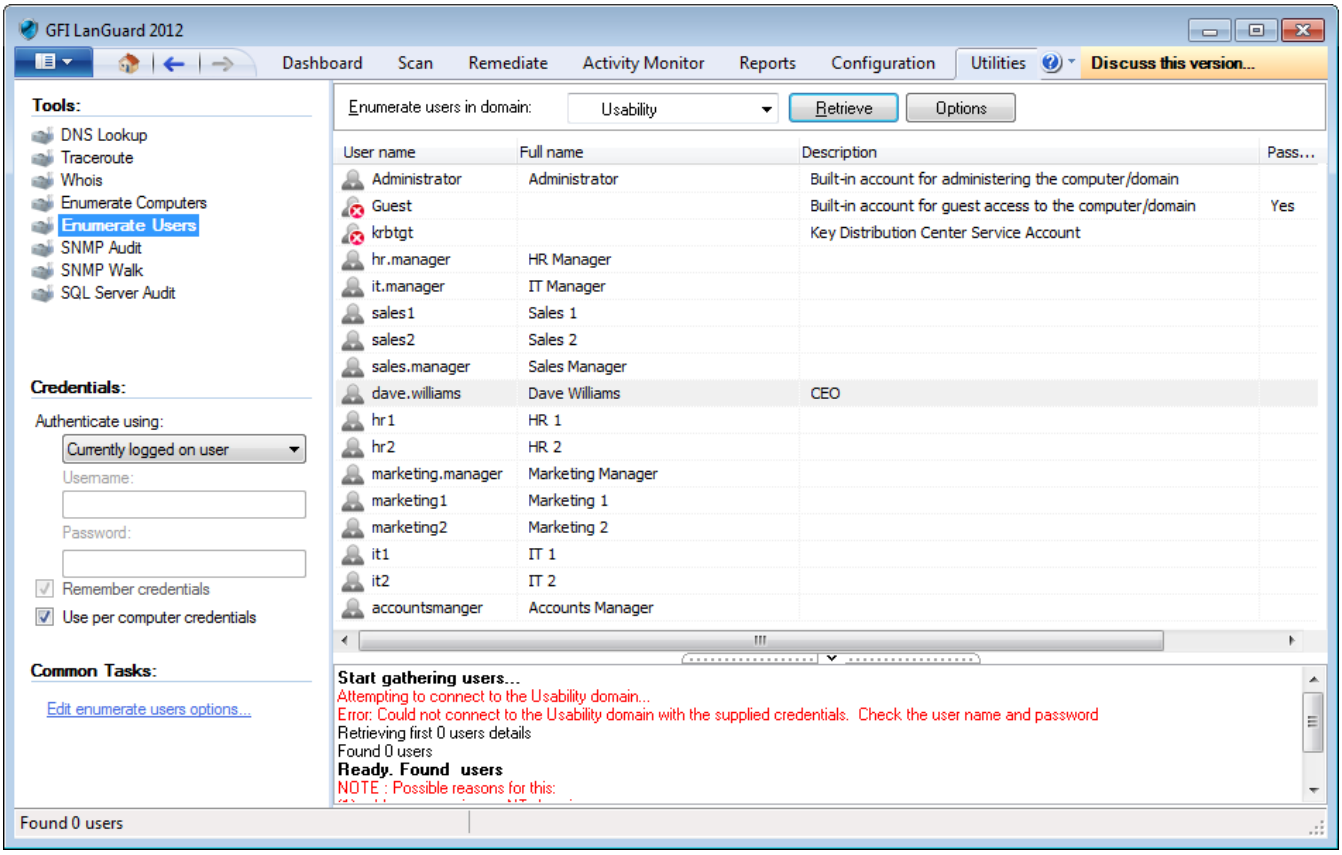
13.4.3 Enabling Auditing Policies

The Enumerate Computers tool also enables you to configure auditing policies on particular computers. This is done as follows:

1. Select the computers on which you want to enable auditing policies.

2. Right-click on any of the selected computers and select **Enable Auditing Policies**. This will launch the **Auditing Policies configuration Wizard** that will guide you through the configuration process.

13.5 Enumerate Users



Screenshot 152: The Enumerate Users tool dialog

To scan the Active Directory® and retrieve the list of all users and contacts included in this database:

1. Launch GFI LanGuard.

2. Click **Utilities** tab and select **Enumerate Users** in the left pane under **Tools**.

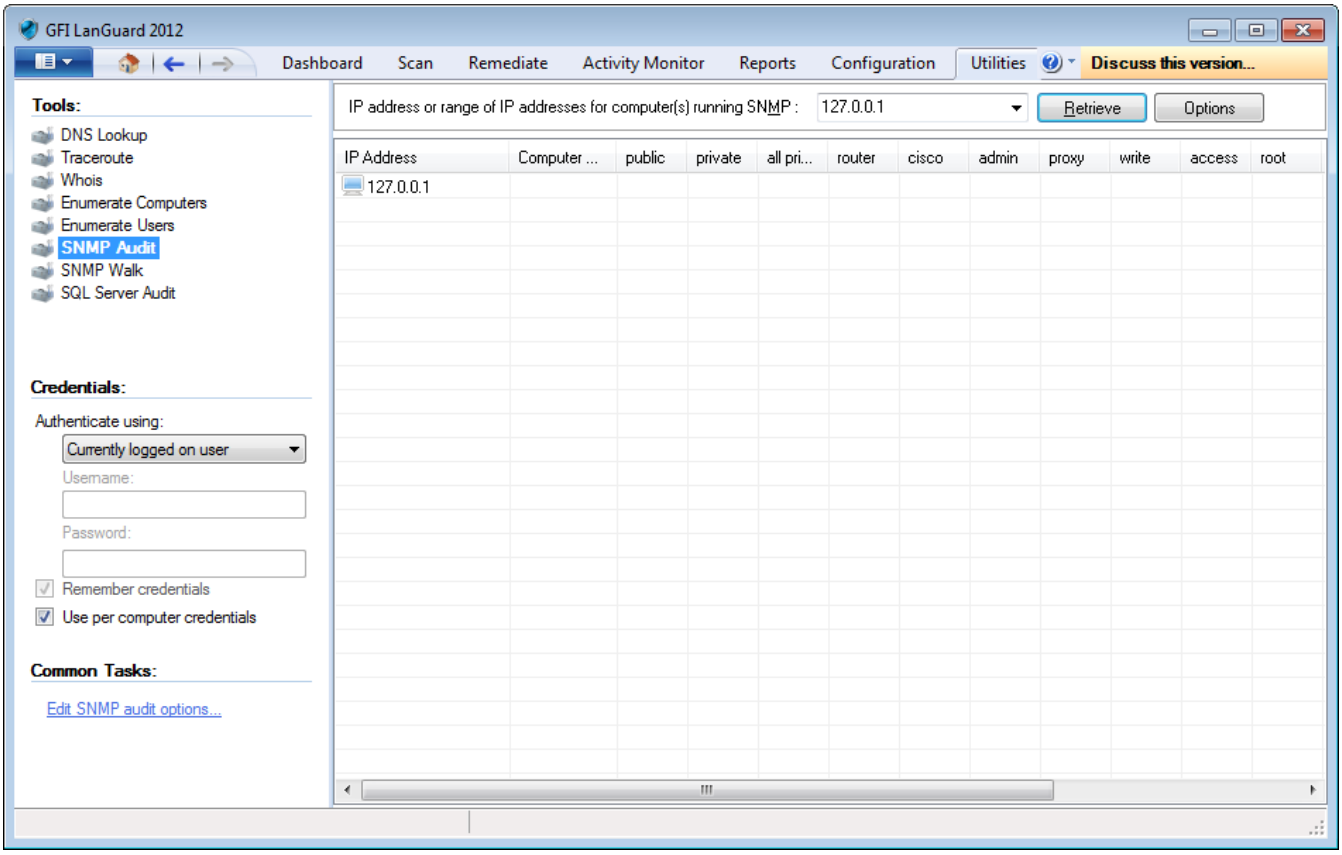
3. In the **Enumerate users in domain** menu, select the desired domain.

4. From **Common Tasks** in the left pane, click **Edit Enumerate Users options** or **Options** on the right pane to filter the information to extract and display only the users or contacts details. In addition, you can optionally configure this tool to highlight disabled or locked accounts.

5. Click **Retrieve** to start the process.

> **Note**
>
> This tool can enable or disable enumerated user accounts. Right-click on the account and select **Enable/Disable account** accordingly.

13.6 SNMP Auditing



Screenshot 153: SNMP Audit tool

This tool identifies and reports weak SNMP community strings by performing a dictionary attack using the values stored in its default dictionary file (snmp-pass.txt).

You can add new community strings to the default dictionary file by using a text editor (for example, notepad.exe).

You can also direct the SNMP Audit tool to use other dictionary files. To achieve this, specify the path to the dictionary file that you want to from the tool options at the right of the management console.

To perform SNMP audits on network targets and identify weak community strings:

1. Launch GFI LanGuard.

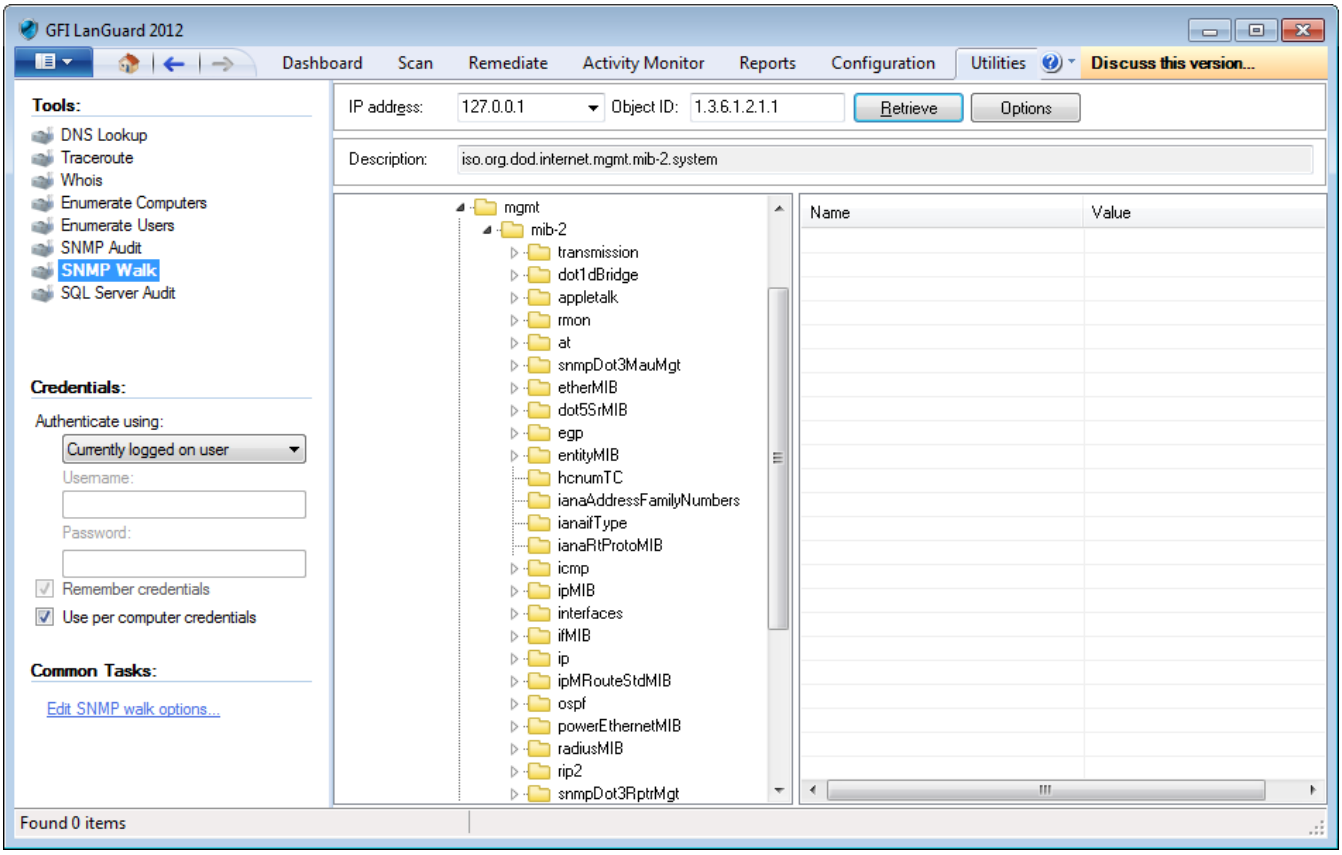
2. Click **Utilities** tab and select **SNMP Audit** in the left pane under **Tools**.

3. In the **IP of computer running SNMP**, specify the IP to reach.

4. From **Common Tasks** in the left pane, click on **Edit SNMP Audit options** or **Options** on the right pane to edit the default options.

5. Click **Retrieve** to start the process.

13.7 SNMP Walk



Screenshot 154: SNMP Walk tool

To probe your network nodes and retrieve SNMP information (for example, OID's):

1. Launch GFI LanGuard.

2. Click **Utilities** tab and select SNMP Walk in the left pane under **Tools**.

3. In the **IP address** menu, specify the IP address of the computer that you wish to scan for SNMP information.

4. From **Common Tasks** in the left pane, click **Edit SNMP Walk options** or **Options** on the right pane to edit the default options such as providing alternative community strings.

5. Click **Retrieve** to start the process.

IMPORTANT

SNMP activity is normally blocked at the router / firewall so that internet users cannot SNMP scan your network. Malicious users can use information enumerated through SNMP scanning to hack your network / systems. Unless this service is required, it is highly recommended to disable it.

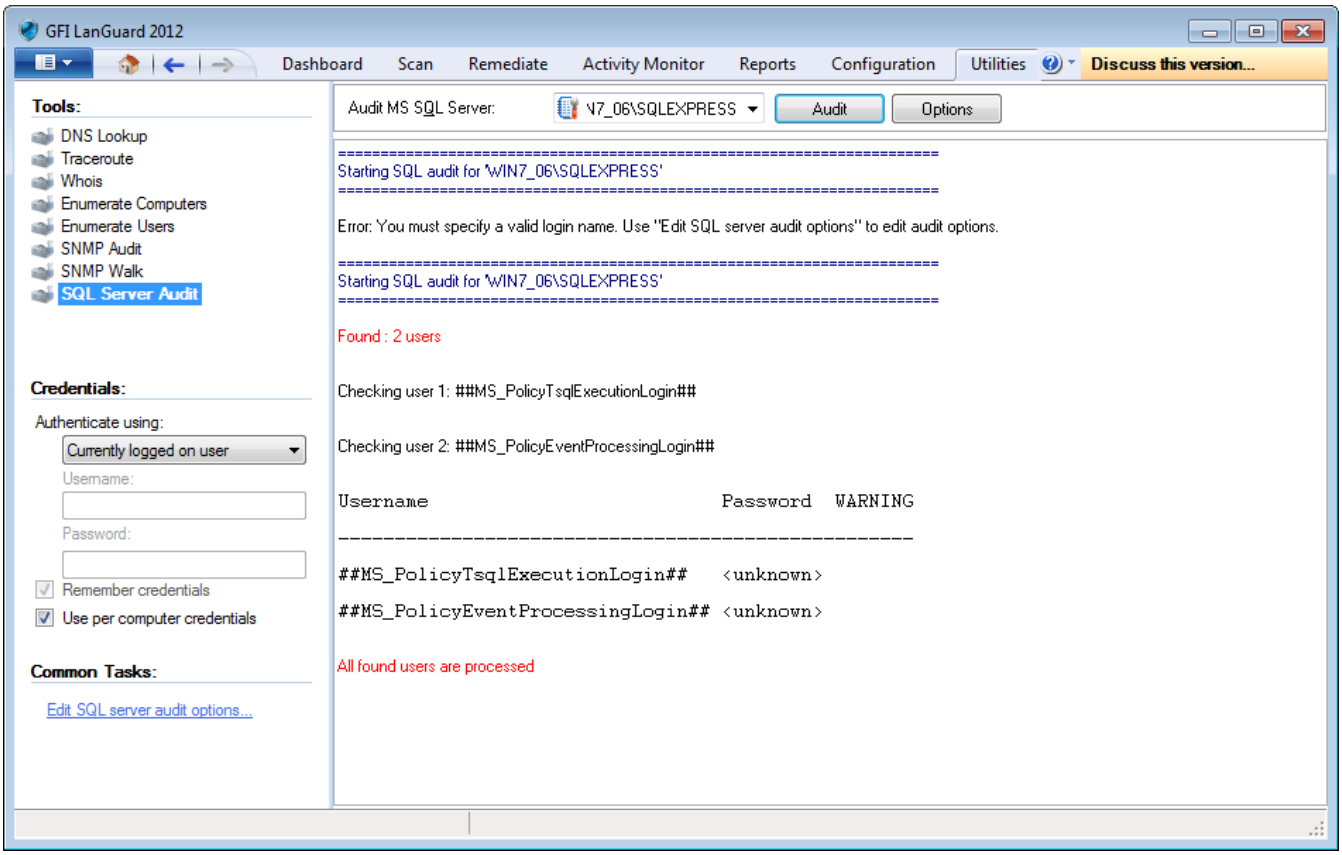
13.8 SQL Server® Audit

This tool enables you to test the password vulnerability of the 'sa' account (i.e. root administrator), and any other SQL user accounts configured on the SQL Server®. During the audit process, this tool will perform dictionary attacks on the SQL Server® accounts using the credentials specified in the 'passwords.txt' dictionary file. However, you can also direct the SQL Server® Audit tool to use other dictionary files. You can also customize your dictionary file by adding new passwords to the default list.

To perform a security audit on a particular SQL Server® installation:

1. Launch GFI LanGuard.

2. Click **Utilities** tab and select **SQL Server Audit** in the left pane under **Tools**.



Screenshot 155: SQL Server® Audit

3. In the **Audit MS SQL Server** menu, specify the IP address of the SQL Server® that you wish to audit.

4. From **Common Tasks** in the left pane, click **Edit SQL Server® Audit options** or **Options** button on the right pane to edit the default options such as performing dictionary attacks on all the other SQL user accounts.

5. Click **Audit** to start the process.

13.9 Command Line Tools

The command line tools enable you to launch network vulnerability scans and patch deployment sessions as well as importing and exporting profiles and vulnerabilities without loading up the GFI LanGuard management console. Use the information in this section to learn how to run patch management functions using the following CMD tools:

- Lnsscmd.exe
- Deploycmd.exe
- Impex.exe

13.9.1 Using lnsscmd.exe

The 'lnsscmd.exe' command line target-scanning tool allows you to run vulnerability checks against network targets directly from the command line, or through third party applications, batch files and scripts. The 'lnsscmd.exe' command line tool supports the following switches:

```
lnsscmd <Target> [/profile=profileName] [/report=reportPath]
[/reportname=reportName] [/output=pathToXmlFile] [/user=username
/password=password] [/Email [/EmailAddress=EmailAddress]]
[/DontShowStatus] [/UseComputerProfiles] [/Wake] [/Shutdown
[/ShutdownIntervalStart=<hh:mm:ss>] [/ShutdownIntervalEnd=<hh:mm:ss>]]
[/?]
```

lnsscmd command switches

Table 85: lnsscmd command switches

Switch	Description
Target	Specify the IP / range of IPs or host name(s) to be scanned.
/Profile	(Optional) Specify the scanning profile that will be used during a security scan. If this parameter is not specified, the scanning profile that is currently active in the GFI LanGuard will be used. **Note** In the management console, the default (i.e. currently active) scanning profile is denoted by the word (Active) next to its name. To view which profile is active expand the **Configuration** tab > **Scanning Profiles** node.
/Output	(Optional) Specify the full path (including filename) of the XML file where the scan results will be saved.
/Report	(Optional) Directory or full file name for the output scan report.
/ReportName	(Optional) Name of the report to generate. If not specified, the report is saved with a default name.
/User and /Password	(Optional) Specify the alternative credentials that the scanning engine will use to authenticate to a target computer during security scanning. Alternatively you can use the /UseComputerProfiles switch to use the authentication credentials already configured in the dashboard.
/Email	(Optional) Send the resulting report by e-mail. The e-mail address and mail server specified in **Configuration > Alerting Options** are used.
/EmailAddress	(Optional) Dependent on **/Email**. Overrides the general alerting options and uses the specified email address.
/DontShowStatus	(Optional) Include this switch if you want to perform silent scanning. In this way, the scan progress details will not be shown.
/UseComputerProfiles	(Optional) Use per computer credentials when available.
/Wake	(Optional) Wake up offline computers.

Switch	Description
/Shutdown	(Optional) Shuts down computers after scan.
/ShutdownIntervalStart	(Optional) Dependent on **/Shutdown**. The start time of the interval when shutdown is allowed. Use hh:mm:ss format.
/ShutdownIntervalEnd	(Optional) Dependent on **/Shutdown**. The end time of the interval when shutdown is allowed. Use hh:mm:ss format.
/?	(Optional) Use this switch to show the command line tool usage instructions.

Note

Always enclose full paths and profile names within double quotes. For example, `"[path or path name]"` or `"C:\temp\test.xml"`.

The command line target-scanning tool allows you to pass parameters through specific variables. These variables will be automatically replaced with their respective value during execution. The table below describes the supported variables:

Supported variables

Table 86: Supported variables in lnssmcd

Variable	Description
%INSTALLDIR%	During scanning, this variable will be replaced with the path to the GFI LanGuard installation directory.
%TARGET%	During scanning this variable will be replaced with the name of the target computer.
%SCANDATE%	During scanning this variable will be replaced with the date of scan.
%SCANTIME%	During scanning this variable will be replaced with the time of scan.

Example

1. To perform a security scan on a target computer having IP address '130.16.130.1'.
2. Output the scan results to `'c:\out.xml'` (i.e. XML file).
3. Generate a PDF report and save it in `'c:\result.odf'`.
4. Send the PDF report via email to 'lanss@domain.com'

The command should be as follows:

```
lnsscmd.exe 130.16.130.1 /Profile="Default" /Output="c:\out.xml"
/Report="c:\result.pdf" /Email /emailAddress="lanss@domain.com"
```

13.9.2 Using deploycmd.exe

The 'deploycmd.exe' command line patch deployment tool allows you to deploy Microsoft® patches and third party software on remote targets directly from the command line, or through third party applications, batch files or scripts. The 'deploycmd.exe' command line tool supports the following switches:

```
deploycmd <target> </file=FileName> [/switches=Switches]
[/username=UserName /password=Password] [/warnuser] [/userapproval]
[/stopservices] [/customshare=CustomShareName] [/reboot]
[/rebootuserdecides] [/wake] [/shutdown] [/deletefiles] [/timeout=Timeout
(sec)] [/usecomputerprofiles] [/RebootCountdown=Time(sec)]
[/RebootCountdownMessage="Custom message"][/RebootAtFirstOccurenceOf=Time
(formatted as "hh:mm:ss")] [/ShutDownAtFirstOccurenceOf=Time(formatted as
```

```
"hh:mm:ss")] [/RebootInInterval] [/ShutDownInInterval]
[/RebootIntervalStart=Time(formatted as "hh:mm:ss")]
[/RebootIntervalEnd=Time(formatted as "hh:mm:ss")] [/?]
```

deploycmd command switches

Table 87: deploycmd command switches

Switch	Description
Target	Specify the name(s), IP or range of IPs of the target computer(s) on which the patch (es) will be deployed.
/File	Specify the file that you wish to deploy on the specified target(s).
/User and /Password	(Optional) Specify the alternative credentials that the scanning engine will use to authenticate to a target computer during patch deployment. Alternatively you can use the /UseComputerProfiles switch to use the authentication credentials already configured in the Dashboard.
/warnuser	(Optional) Include this switch if you want to inform the target computer user that a file/patch installation is in progress. Users will be informed through a message dialog that will be shown on screen immediately before the deployment session is started.
/useraproval	(Optional) Include this switch to request the user's approval before starting the file/patch installation process. This allows users to postpone the file/patch installation process for later (for example, until an already running process is completed on the target computer).
/stopservice	(Optional) Include this switch if you want to stop specific services on the target computer before installing the file/patch. **Note** You cannot specify the services that will be stopped directly from the command line tool. Services can only be added or removed through the management console.
/customshare	(Optional) Specify the target share where you wish to transfer the file before it is installed.
/reboot	(Optional Parameter) Include this switch if you want to reboot the target computer after file/patch deployment.
/rebootuserdecides	(Optional Parameter) Include this switch to allow the current target computer user to decide when to reboot his computer (after patch installation).
/wake	Wakes up offline computers.
/shutdown	(Optional Parameter) Include this switch if you want to shut down the target computer after the file/patch is installed.
/deletefiles	(Optional Parameter) Include this switch if you want to delete the source file after it has been successfully installed.
/timeout	(Optional Parameter) Specify the deployment operation timeout. This value defines the time that a deployment process will be allowed to run before the file/patch installation is interrupted.
/usecomputerprofiles	(Optional) Use data from computer profiles.
/RebootCountdown	(Optional) Display a reboot countdown window for a number of seconds to the remote user before rebooting.
/RebootCountdownMessage	(Optional) Used in conjunction with **/RebootCountdown**. Displays a custom message to the remote user before rebooting the computer.
/RebootAtFirstOccurenceOf	(Optional) Reboot a computer at the first occurrence of a specified time. The time is expected in the 24 hour format "hh:mm:s s". Example, 18:30:00.
/ShutDownAtFirstOccurenceOf	(Optional) Shutdown a computer at the first occurrence of a specified time. The time is expected in the 24 hour format "hh:mm:s s". Example, 18:30:00.
/RebootInInterval	(Optional) Reboot the computer after deployment if deployment completes in the specified time interval. Otherwise wait to specify the interval manually. Requires parameters `/RebootIntervalStart` and `/RebootIntervalEnd`.

Switch	Description
/ShutdownIntervalStart	(Optional) Dependent on **/Shutdown**. The start time of the interval when shutdown is allowed. Use hh:mm:ss format.
/ShutdownIntervalEnd	(Optional) Dependent on **/Shutdown**. The end time of the interval when shutdown is allowed. Use hh:mm:ss format.
/ShutDownInInterval	(Optional) Shutdown the computer after deployment if deployment completes in the specified time interval. Otherwise wait to specify the interval manually.
/?	(Optional) Use this switch to show the command line tool's usage instructions.

Example

1. Deploy a file called 'patchA001002.XXX'.

2. On target computer 'TMJohnDoe'.

3. Reboot the target computer after successful deployment of the file.

The command should be as follows::

```
deploycmd TMJohnDoe /file="patchA001002.XXX" /reboot
```

13.9.3 Using impex.exe

The Impex tool is a command line tool that can be used to Import and Export profiles and vulnerabilities from GFI LanGuard Network Security Scanner. The parameters supported by this tool are the following:

```
impex [[/H] | [/?]] | [/XML:xmlfile [/DB:dbfile] [[/EX] [/MERGE]] | [/IM
[/ONLYNEWER]] [/PROFILES | /VULNS | /PORTS | /PROFILE:name | /VULNCAT:cat
[/VULN:name] | /PORTTYPE:type [/PORT:number]] [/SKIP | /OVERWRITE |
/RENAME:value]]
```

impex command switches

Table 88: impex command switches

Switch	Description
/H **/?** **Run impex without parameters**	Displays help information.
/XML:<xmlfile>	This parameter specifies the name of the imported or exported XML file. <xmlfile> needs to be replaced with the name of the file the profile is being exported to. **Note** This parameter is mandatory to import or export alerts.
/DB:<dbfile>	Where <dbfile> is the database file to be used during the import/export operation. If this is not specified the default "operationsprofiles.mdb" file will be used.
/EX	Exports data from database to XML file (Default option)
/MERGE	If this is specified when the target XML for export already exists, the file will be opened and data will be merged; otherwise the XML file is first deleted.
/IM	Imports data from XML file to database
/ONLYNEWER	When specified only vulnerabilities newer than the newest vulnerability in the database will be imported.
/PROFILES	Exports/Imports all scanning profiles.
/VULNS	Exports/Imports all vulnerabilities.
/PORTS	Exports/Imports all ports
/PROFILE:<name>	Exports/Imports the specified scanning profile.

Switch	Description
/VULNCAT:<category>	Exports/Imports all vulnerabilities of the specified category.
/VULN:<name>	Exports/Imports the specified vulnerability (/VULNCAT must be specified).
/PORTTYPE:<type>	Exports/Imports all ports of the specified type.
/PORT:<number>	Exports/Imports the specified port (/PORTTYPE must be specified).
/SKIP	If an item already exists in the target XML/database, that item will be skipped
/OVERWRITE	If an item already exists in the target XML/database, that item will be overwritten.
/RENAME:<value>	If an item already exists in the target XML/database, that item will be renamed to <value>. If /PROFILE or /VULN was specified, port information merged with that item is a port or renamed by prefixing its name with <value> in any other case.

Example 1

To import specific entries from an XML file:

```
impex /xml:regcheck.xml /vuln:"Blaster Worm" /vulncat:"Registry
Vulnerabilities"
```

Example 2

To import a whole XML file:

```
impex /xml:regcheck.xml /im
```

Note

The Impex executable can be located in the GFI LanGuard installation folder.

Note

If the specified `<xmlfile>`, `<dbfile>`, `<name>`, `<category>` or `<value>` contain any space character, the whole value must be placed between double quotes. Example:

- `<xmlfile>` containing space = `"Vulnerability Checks Definitions.xml"`
- `<xmlfile>` without space = `VulnerabilityChecksDefinitions.xml`

Note

It is recommended that if the vulnerabilities are imported into another installed instance of GFI LanGuard; that installation will have the same build number as the one the database has been exported from.

IMPORTANT

It is highly recommended not to use the **Impex** tool if GFI LanGuard application (LanGuard.exe) or LanGuard scanning profiles (scanprofiles.exe) are running.

14 Script Debugger

Scripts that identify custom vulnerabilities can be created using any VBScript compatible scripting language. By default, GFI LanGuard ships with a script editor that you can use to create your custom scripts.

New checks must be included in the list of checks supported by GFI LanGuard. Use the Vulnerability Assessment tab to add new checks to the default list of vulnerability checks on a scan profile by scan profile basis. GFI LanGuard also supports Python scripting.

Topics in this chapter:

14.1 Creating custom scripts using VBscript 228

14.2 Creating custom scripts using Python Scripting 233

14.3 SSH Module 237

14.1 Creating custom scripts using VBscript

GFI LanGuard supports and runs scripts written in VBscript compatible languages. Use VBscript compatible languages to create custom scripts that can be run against your network targets.

Security auditing scripts can be developed using the script editor that ships with GFI LanGuard. This built-in script editor includes syntax highlighting capabilities as well as debugging features that support you during script development. Open the script editor from **Start > Programs > GFI LanGuard > LanGuard Script Debugger**.

Note

1. For more information on how to develop scripts using the built-in script editor, refer to the **Scripting documentation** help file included in **Start > Programs > GFI LanGuard > LanGuard Scripting documentation**.

Note

GFI does not support requests related to problems in custom scripts. You can post any queries that you may have about GFI LanGuard forums at http://forums.gfi.com/. Through this forum, you are able to share scripts, problems and ideas with other GFI LanGuard users.

14.1.1 Adding a vulnerability check that uses a custom VBScript (.vbs)

To create new vulnerability checks that use custom VBScripts, follow the steps described in this section:

- Step 1: Create the script
- Step 2: Add new vulnerability checks
- Step 3: Test the vulnerability check/script

Step 1: Create the script

1. Launch the Script Debugger from **Start > Programs > GFI LanGuard > LanGuard Script Debugger**.

2. Go on **File > New**.

3. Create a script. For this example, use the following sample script code.

```
Function Main
   echo "Script has run successfully"
   Main = true
End Function
```

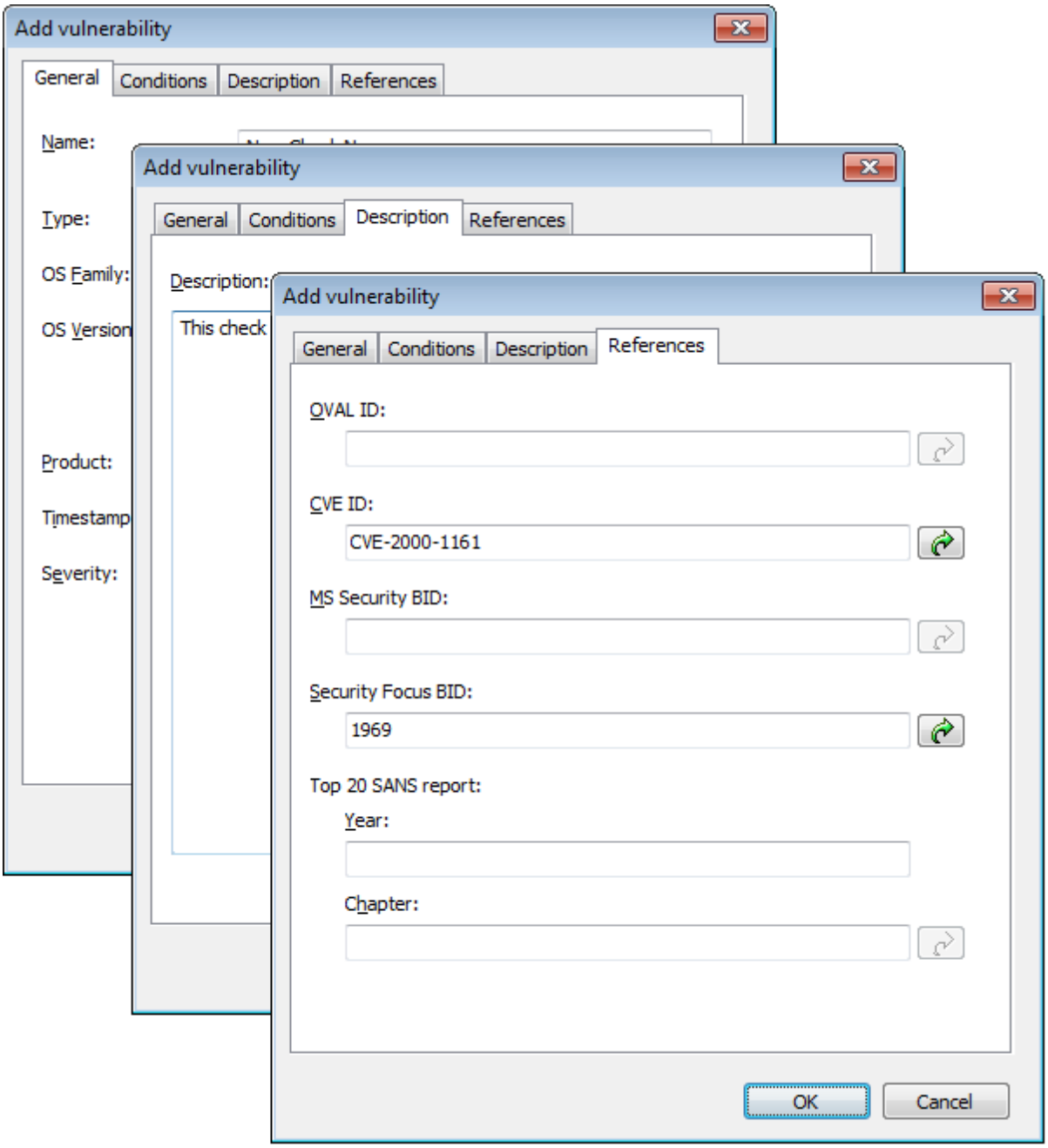
4. Save the script in `<LanGuard installation folder path>\Data\Scripts\myscript.vbs`.

Step 2: Add new vulnerability checks

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

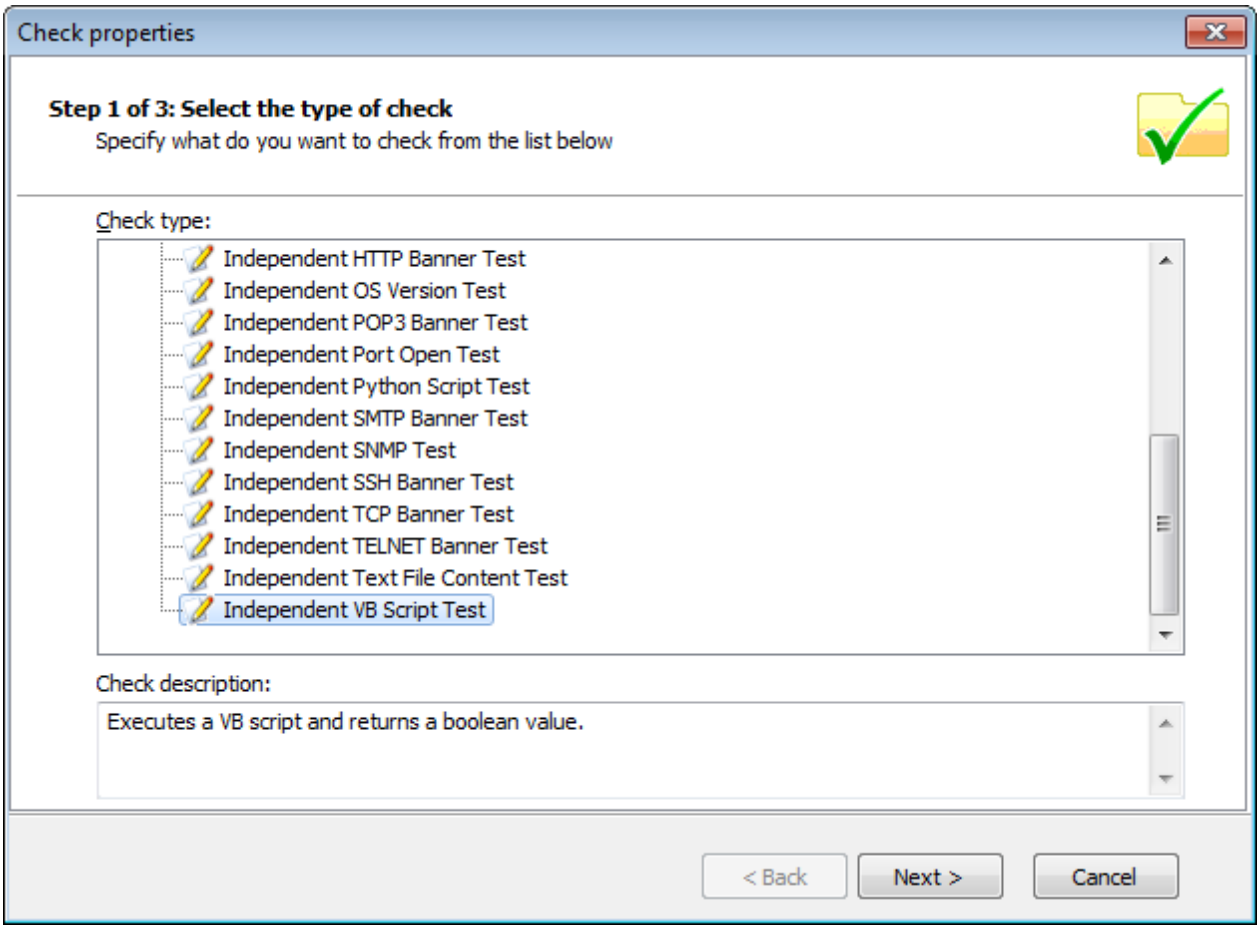
3. In the new window, add a new vulnerability by clicking **Add** under the list of vulnerability checks.



Screenshot 156: Add vulnerability dialog

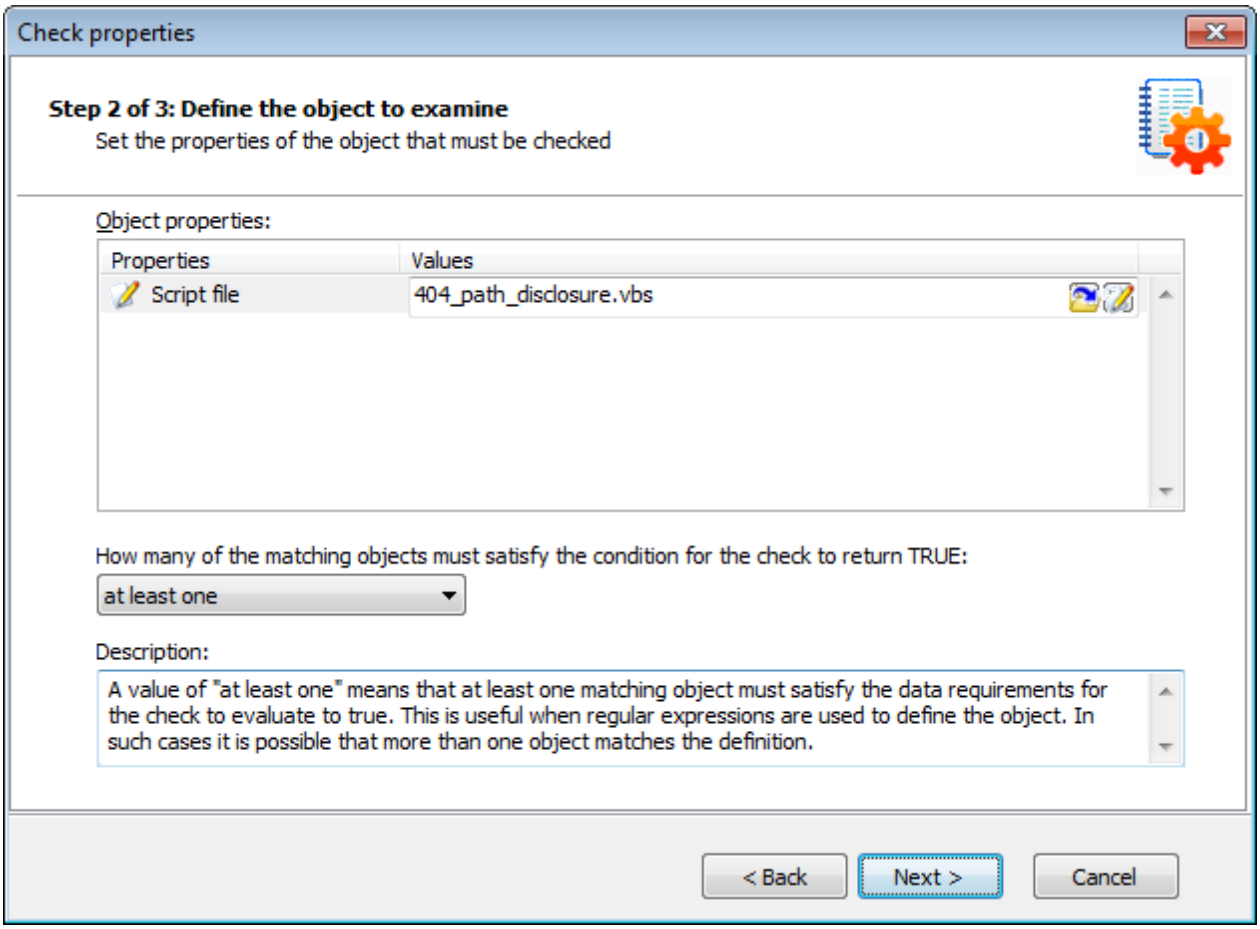
4. Go through the **General**, **Description** and **References** tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

5. Click the **Conditions** tab and click on the **Add** button. This will bring up the check properties wizard.


Check properties
Step 1 of 3: Select the type of check
Specify what do you want to check from the list below
Check type:
Independent HTTP Banner Test
Independent OS Version Test
Independent POP3 Banner Test
Independent Port Open Test
Independent Python Script Test
Independent SMTP Banner Test
Independent SNMP Test
Independent SSH Banner Test
Independent TCP Banner Test
Independent TELNET Banner Test
Independent Text File Content Test
Independent VB Script Test
Check description:
Executes a VB script and returns a boolean value.
< Back
Next >
Cancel

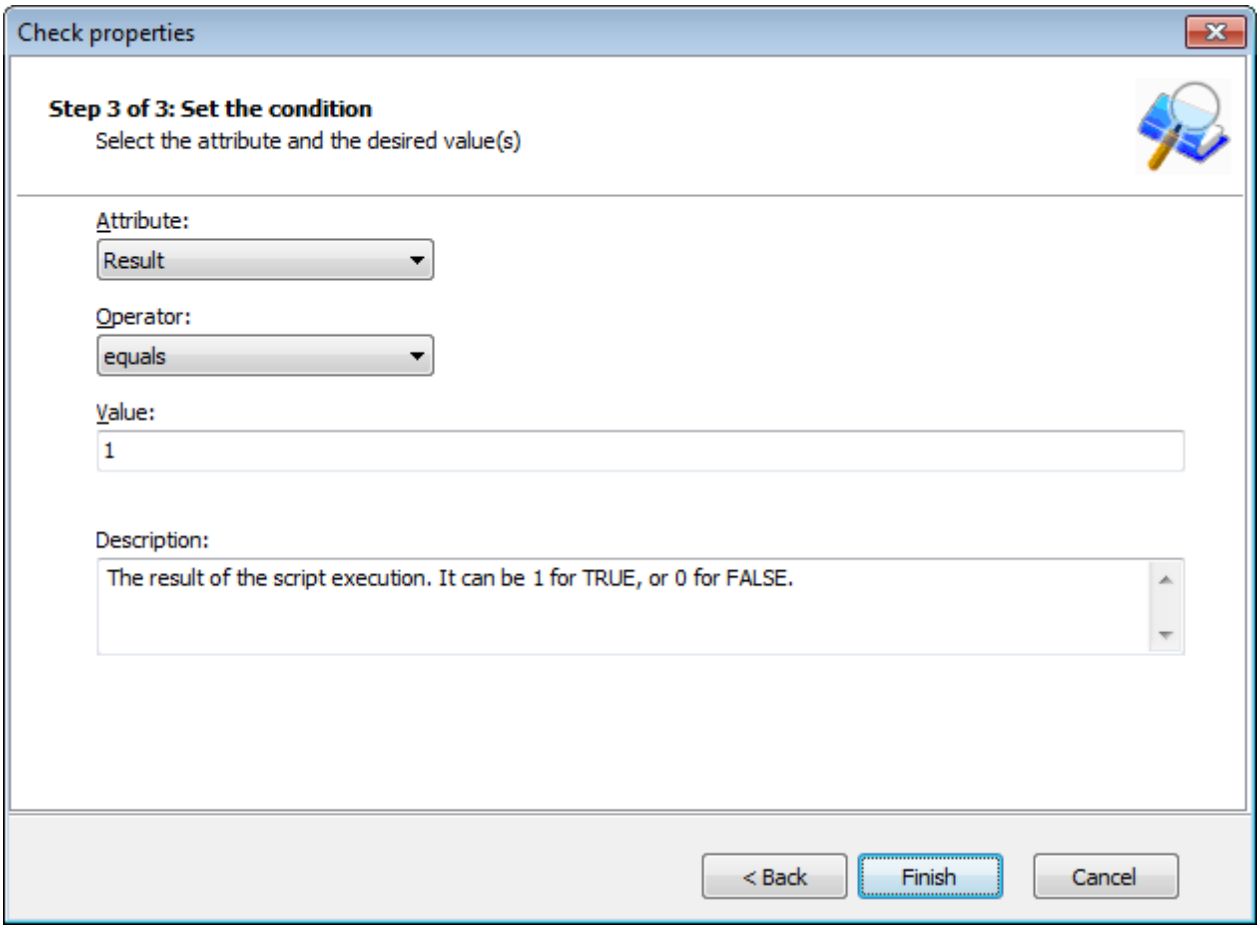
Screenshot 157: Adding vulnerability checks - Select type of check

6. Select **Independent checks > VBScript** node and click **Next.**


Check properties
Step 2 of 3: Define the object to examine
Set the properties of the object that must be checked
Object properties:
Properties
Values
Script file
404_path_disclosure.vbs
How many of the matching objects must satisfy the condition for the check to return TRUE:
at least one
Description:
A value of "at least one" means that at least one matching object must satisfy the data requirements for the check to evaluate to true. This is useful when regular expressions are used to define the object. In such cases it is possible that more than one object matches the definition.
< Back
Next >
Cancel

Screenshot 158: Adding vulnerability checks - Select VB Script file

7. Click **Choose file** and select the custom VBscript file that will be executed by this check. Click **Next**.



Screenshot 159: Adding vulnerability checks - Define conditions

8. Select the relative condition setup in the wizard to finalize script selection. Click Finish to exit wizard.

9. Click **OK** to save new vulnerability check.

Step 3: Test the vulnerability check/script

Scan your local host computer using the scanning profile where the new check was added.

In **Scan** tab > **Results**, a vulnerability warning will be shown in the **Vulnerability Assessment** node of the scan results.

14.2 Creating custom scripts using Python Scripting

GFI LanGuard also supports a new type of vulnerability checks – Python Script Test. This type of check is available under the Independent Checks type.

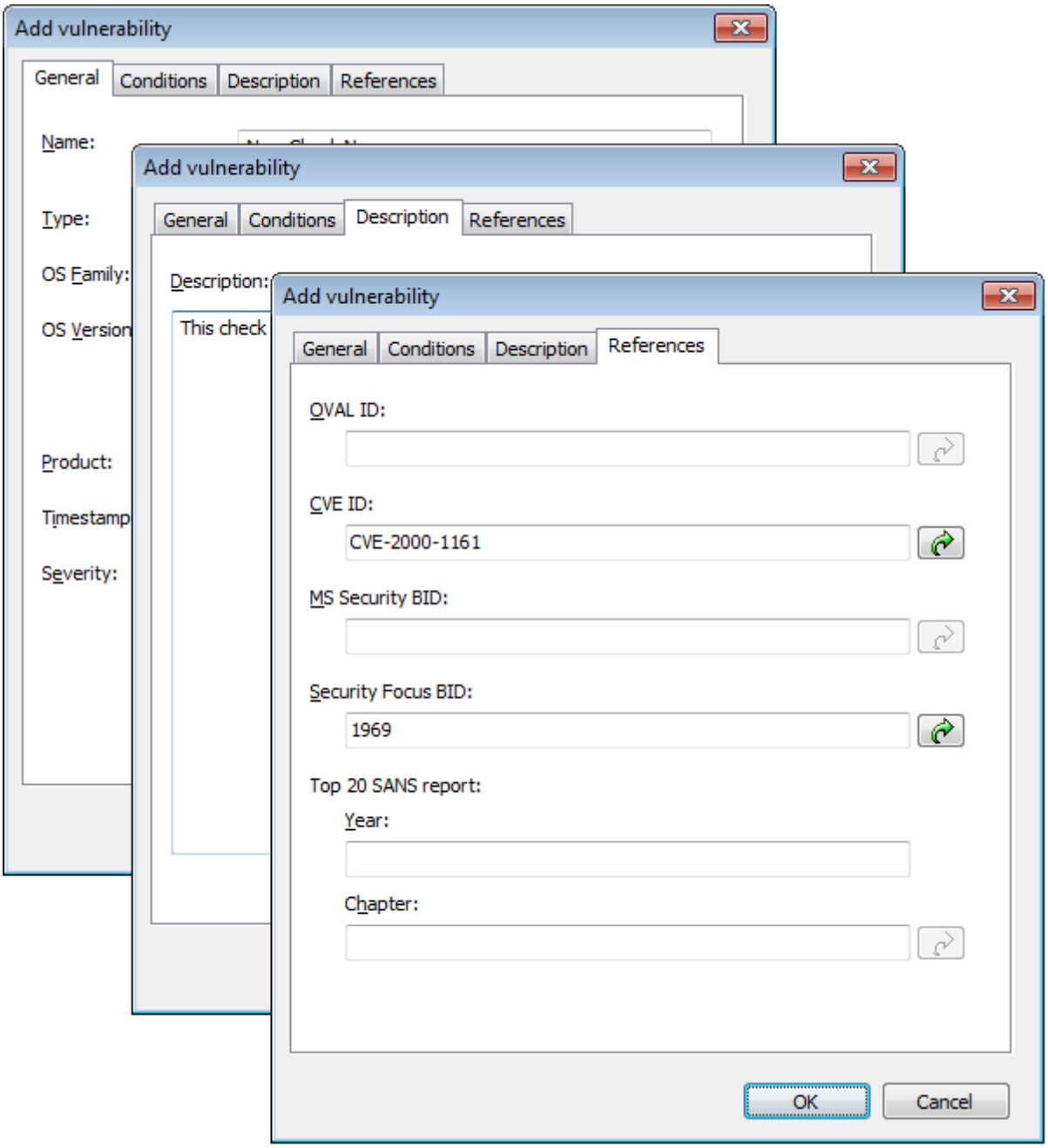
> **Important**
>
> For information about Python Scripting, refer to the GFI LanGuard scripting documentation from **Start > Programs > GFI LanGuard 2012 > GFI LanGuard Scripting Documentation**.

To add a new python script check:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

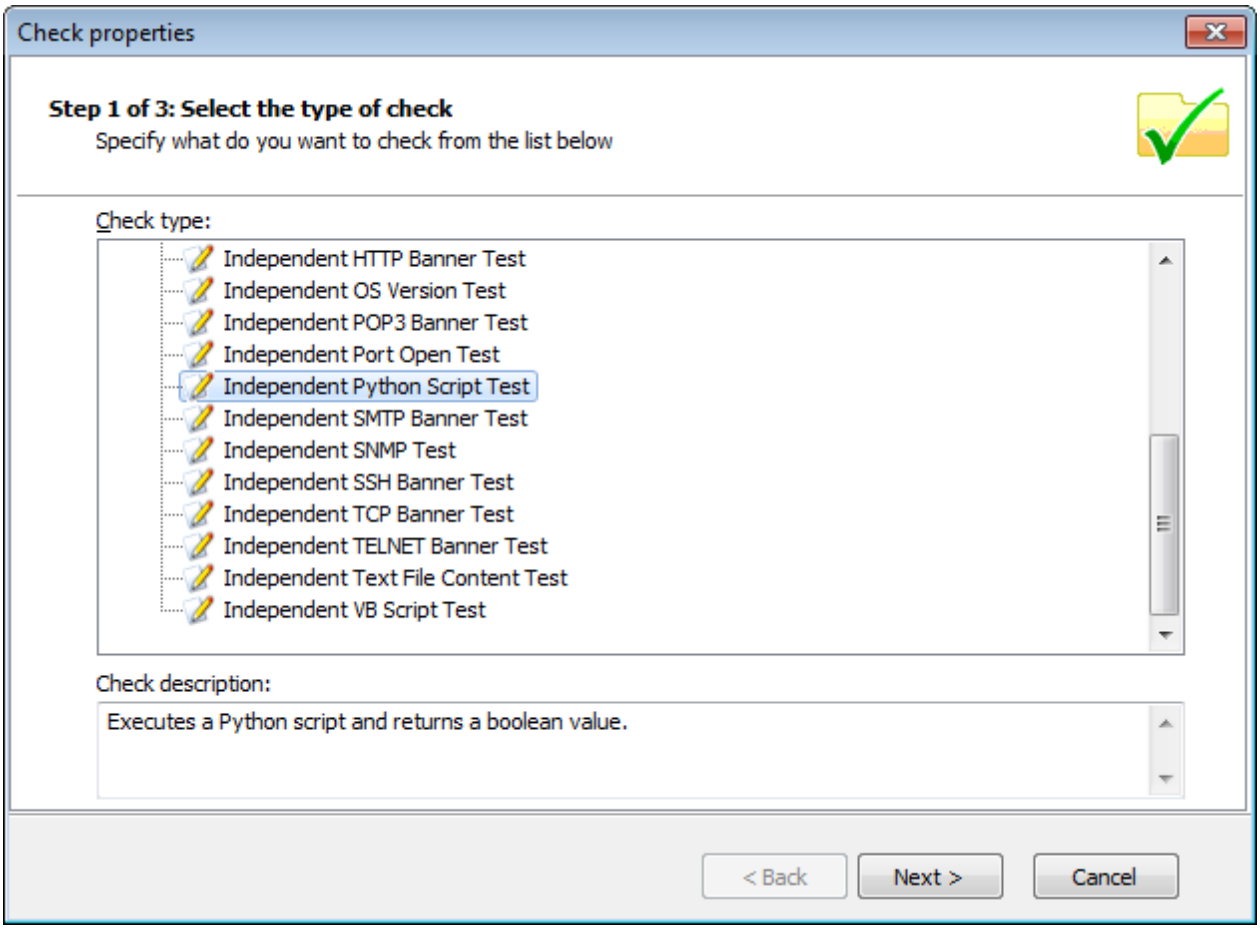
3. In the new window, add a new vulnerability by clicking **Add** under the list of vulnerability checks.



Screenshot 160: Add vulnerability dialog

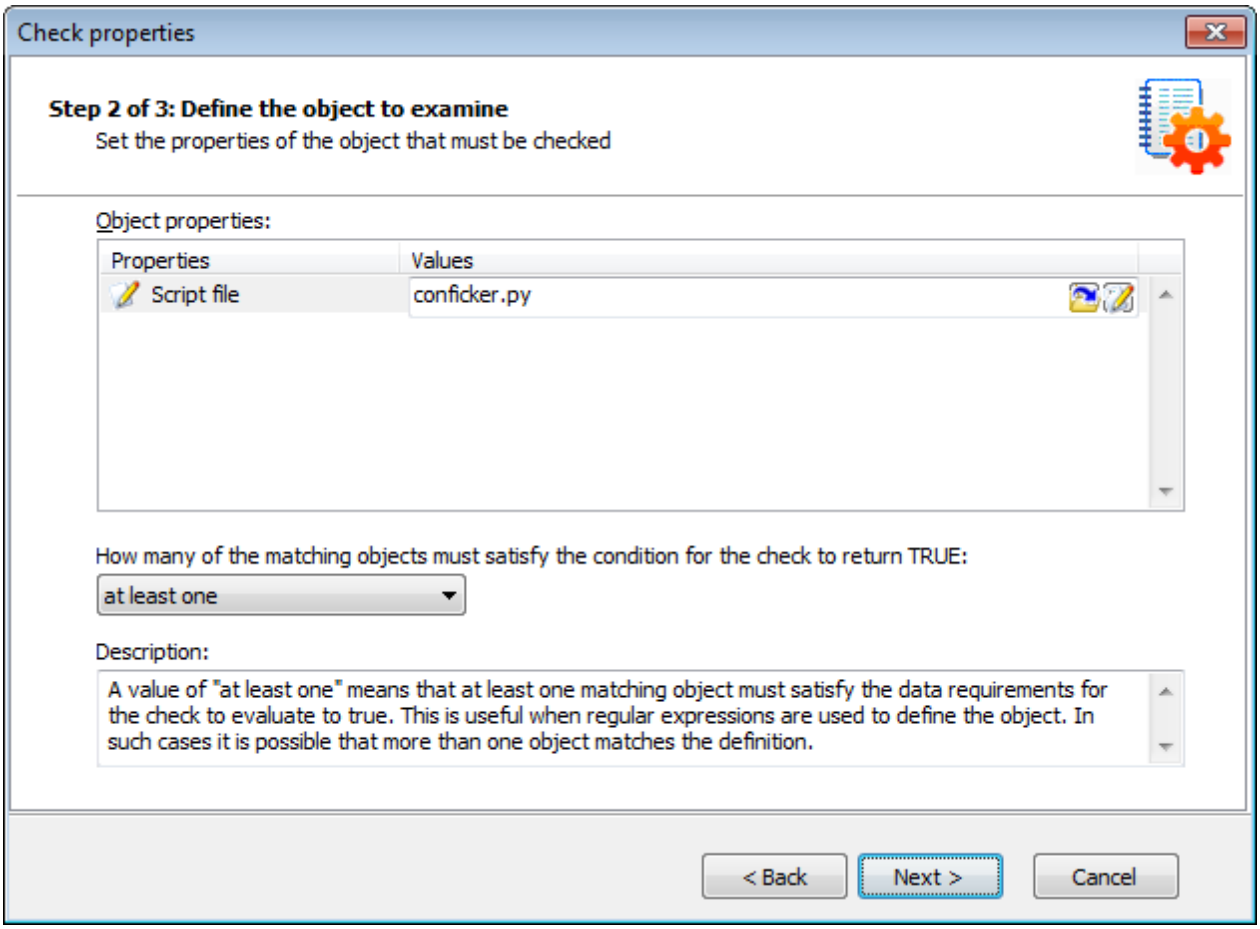
4. Go through the **General**, **Description** and **References** tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

5. Click the **Conditions** tab and click on the **Add** button. This will bring up the check properties wizard.


Check properties
Step 1 of 3: Select the type of check
Specify what do you want to check from the list below
Check type:
Independent HTTP Banner Test
Independent OS Version Test
Independent POP3 Banner Test
Independent Port Open Test
Independent Python Script Test
Independent SMTP Banner Test
Independent SNMP Test
Independent SSH Banner Test
Independent TCP Banner Test
Independent TELNET Banner Test
Independent Text File Content Test
Independent VB Script Test
Check description:
Executes a Python script and returns a boolean value.
< Back
Next >
Cancel

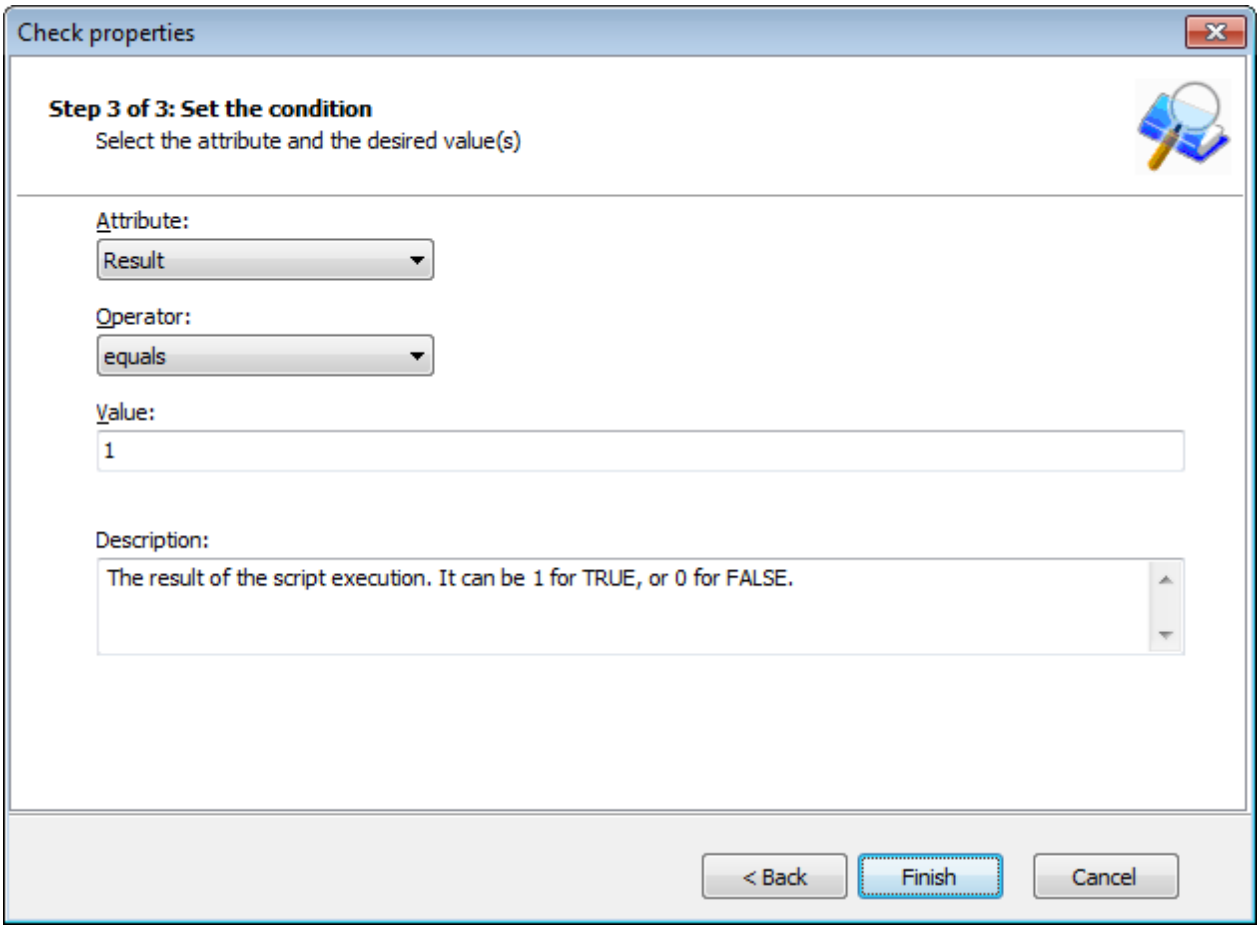
Screenshot 161: Adding vulnerability checks - Select type of check

6. Select **Independent checks > Independent Python Script Test** node and click **Next.**


Check properties
Step 2 of 3: Define the object to examine
Set the properties of the object that must be checked
Object properties:
Properties
Values
Script file
conficker.py
How many of the matching objects must satisfy the condition for the check to return TRUE:
at least one
Description:
A value of "at least one" means that at least one matching object must satisfy the data requirements for the check to evaluate to true. This is useful when regular expressions are used to define the object. In such cases it is possible that more than one object matches the definition.
< Back
Next >
Cancel

Screenshot 162: Adding vulnerability checks - Select Python Script file

7. Click **Choose file** and select the custom Python Script file that will be executed by this check. Click **Next**.



Screenshot 163: Adding vulnerability checks - Defining conditions

8. Select the relative condition setup in the wizard to finalize script selection. Click Finish to exit wizard.

9. Click **OK** to save new vulnerability check.

14.3 SSH Module

GFI LanGuard includes an SSH module which handles the execution of vulnerability scripts on Linux/UNIX based systems.

The SSH module determines the result of vulnerability checks through the console (text) data produced by an executed script. This means that you can create custom Linux/UNIX vulnerability checks using any scripting method that is supported by the target operating system.

14.3.1 Keywords

The SSH module can run security scanning scripts through its terminal window. When a security scan is launched on Linux/UNIX based target computers, vulnerability checking scripts are copied through an SSH connection to the respective target computer and run locally.

The SSH connection is established using the logon credentials (i.e. username and password/SSH Private Key file) specified prior to the start of a security scan.

The SSH module can determine the status of a vulnerability check through specific keywords present in the text output of the executed script. These keywords are processed by the module and interpreted as instruction for the GFI LanGuard. Standard keywords identified by the SSH module include the following:

Table 89: Vulnerability keywords

Keyword	Description
TRUE: / FALSE	These strings indicate the result of the executed vulnerability check/script. When the SSH module detects a TRUE: it means that the check was successful; FALSE: indicates that the vulnerability check has failed.
AddListItem	This string triggers an internal function that adds results to the vulnerability check report (i.e. scan results). These results are shown in the GFI LanGuard management console after completion of a scan. This string is formatted as follows: `AddListItem([[[[parent node]]]],[[[[actual string]]]])`
[[[[parent node]]]]	Includes the name of the scan results node to which the result will be added.
[[[[actual string]]]]	Includes the value that will be added to the scan results node. **Note** Each vulnerability check is bound to an associated scan result node. This means that 'AddListItem' results are by default included under an associated/default vulnerability node. In this way, if the parent node parameter is left empty, the function will add the specified string to the default node.
SetDescription	This string triggers an internal function that will overwrite the default description of a vulnerability check with a new description. This string is formatted as follows: SetDescription([New description])
!!SCRIPT_FINISHED!!	This string marks the end of every script execution. The SSH module will keep looking for this string until it is found or until a timeout occurs. If a timeout occurs before the '!!SCRIPT_FINISHED!!' string is generated, the SSH module will classify the respective vulnerability check as failed. **Note** It is imperative that every custom script outputs the '!!SCRIPT_FINISHED!!' string at the very end of its checking process.

14.3.2 Adding a vulnerability check that uses a custom shell script

In the following example a vulnerability check is created (for Linux based targets) which uses a script written in Bash. The vulnerability check in this example will test for the presence of a dummy file called 'test.file'

Step 1: Create the script

1. Launch your favorite text file editor.

2. Create a new script using the following code:

```
#!/bin/bash
if [ -e test.file ]
then
   echo "TRUE:"
else
   echo "FALSE:"
fi
echo "!!SCRIPT_FINISHED!!"
```

3. Save the file in `<GFI LanGuard 2011 installation folder path>..\Data\Scripts\myscript.sh`

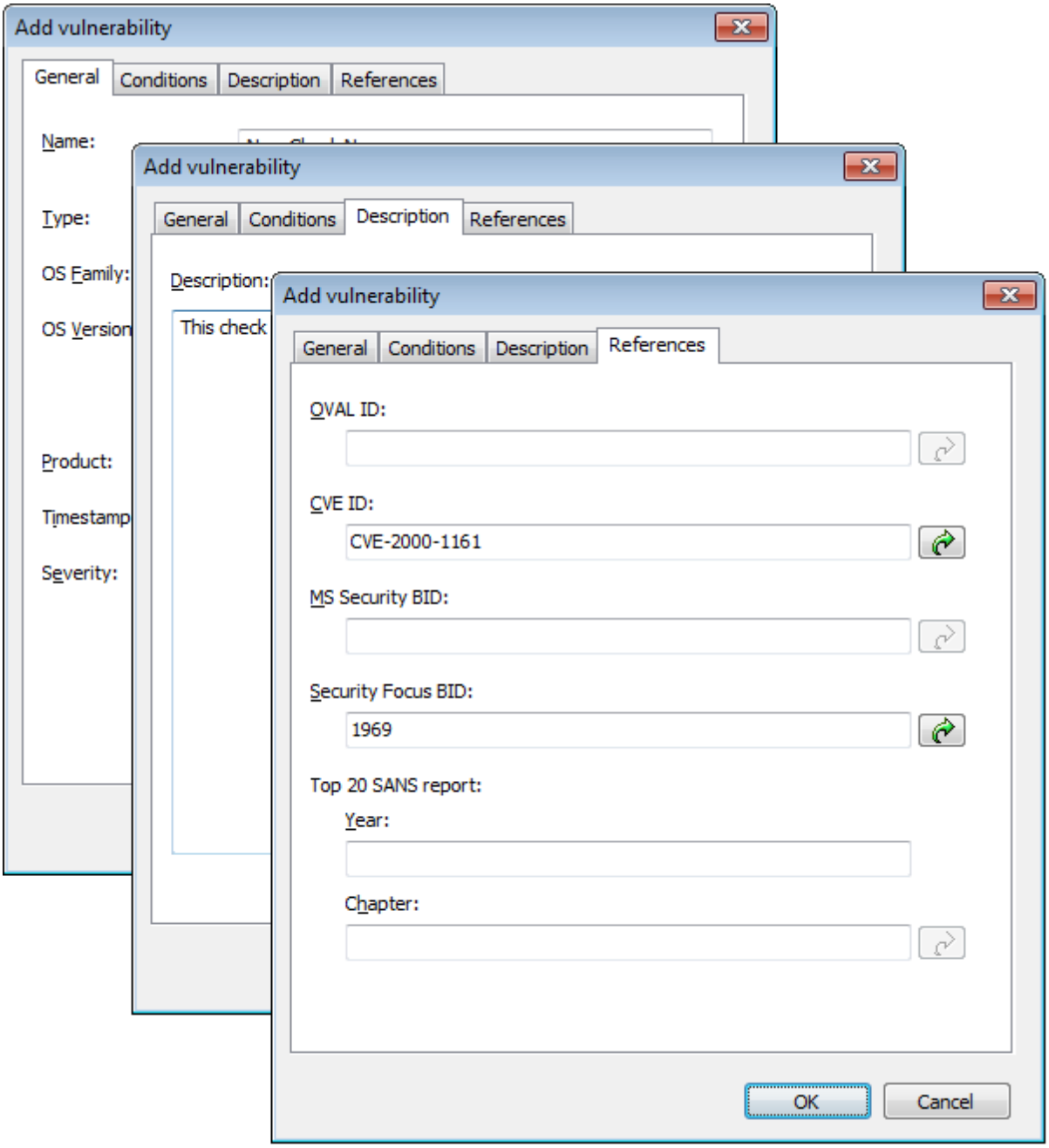
Step 2: Add the new vulnerability check

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

3. From the middle pane, select the category in which the new vulnerability check will be included (for example, High Security Vulnerabilities…).

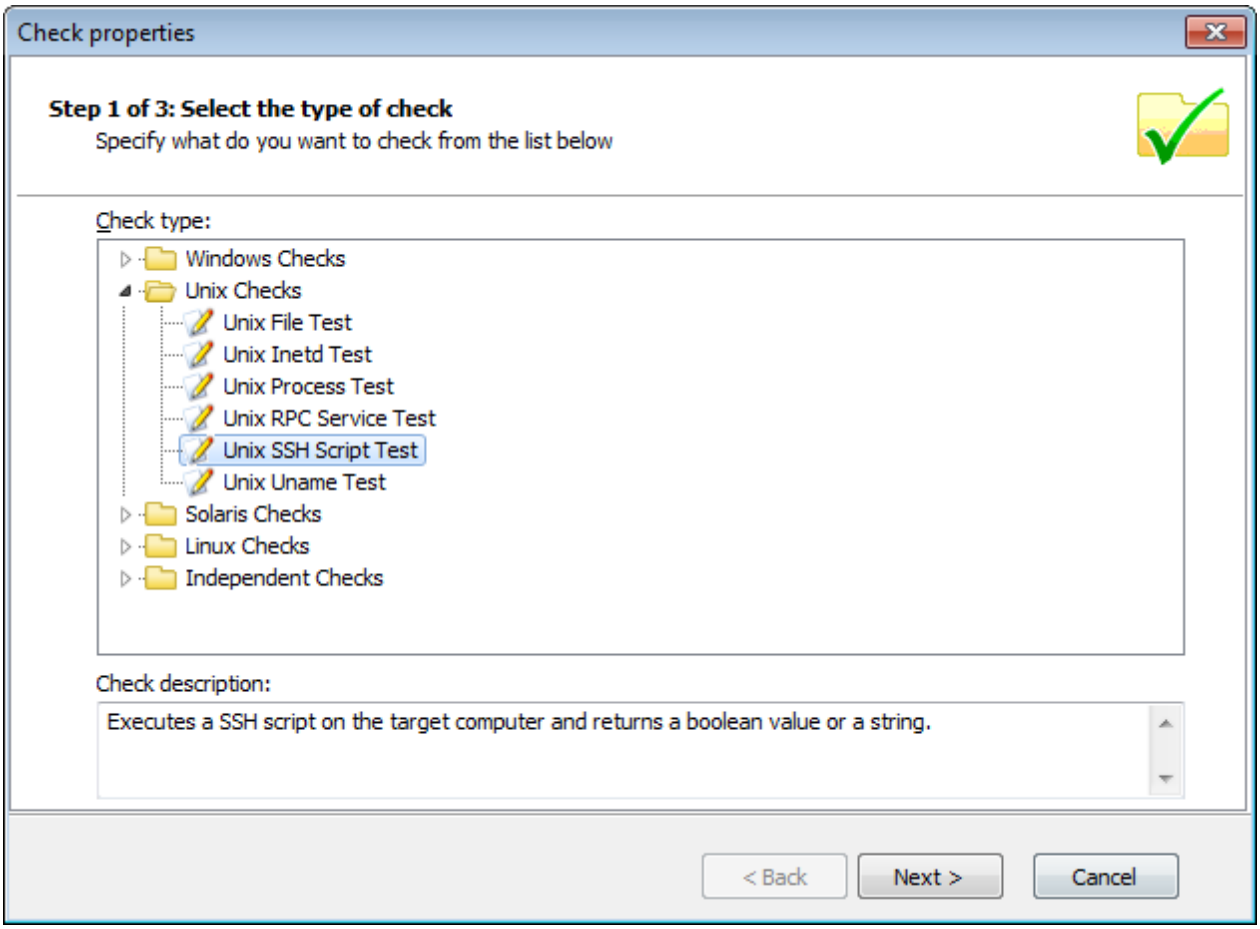
4. In the new window, add a new vulnerability by clicking **Add** in the middle pane.



Screenshot 164: Add vulnerability dialog

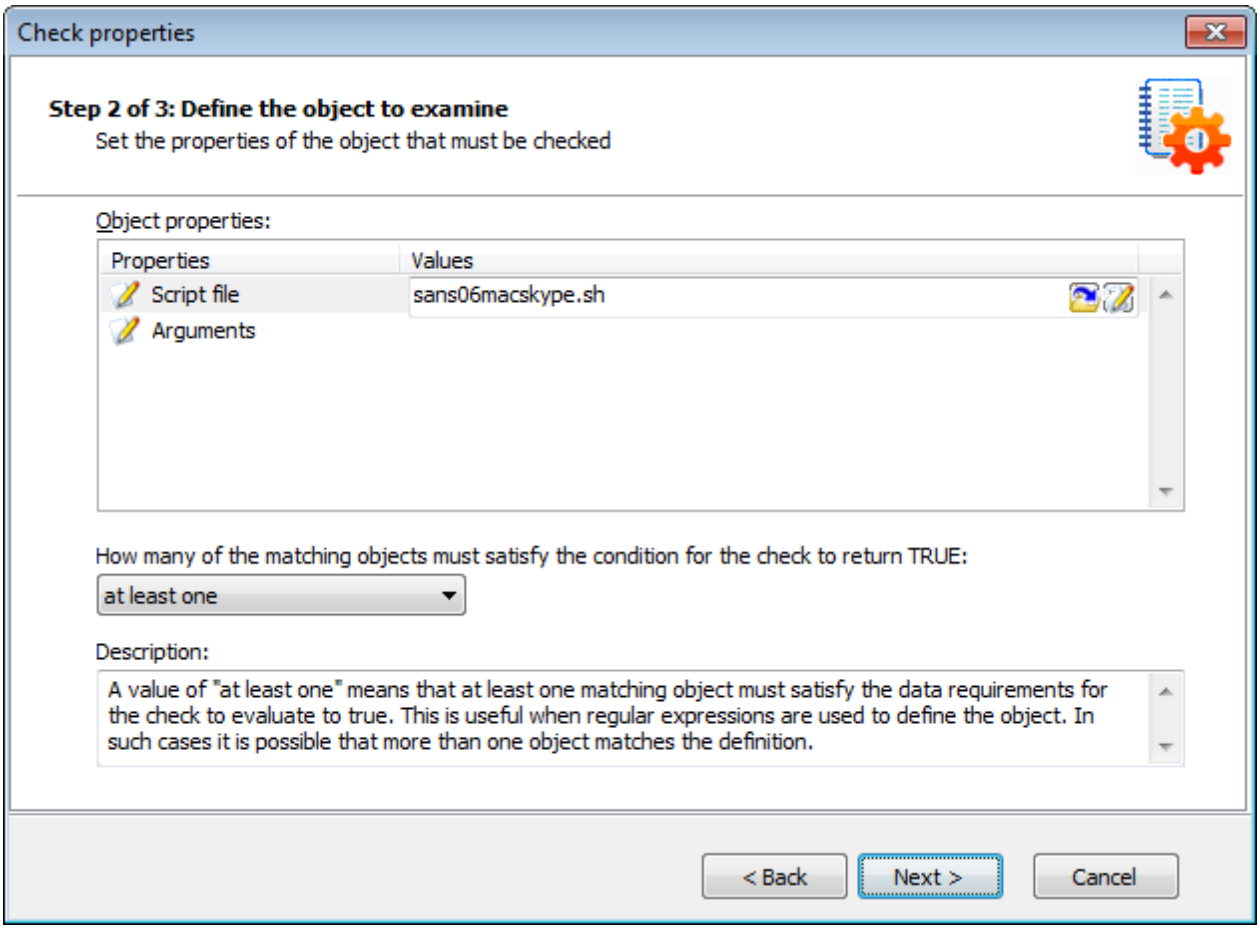
5. Go through the **General**, **Description** and **Reference** tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

6. Choose the **Conditions** tab and click **Add** button. This will bring up the check properties wizard.


Check properties
Step 1 of 3: Select the type of check
Specify what do you want to check from the list below
Check type:
Windows Checks
Unix Checks
Unix File Test
Unix Inetd Test
Unix Process Test
Unix RPC Service Test
Unix SSH Script Test
Unix Uname Test
Solaris Checks
Linux Checks
Independent Checks
Check description:
Executes a SSH script on the target computer and returns a boolean value or a string.
< Back
Next >
Cancel

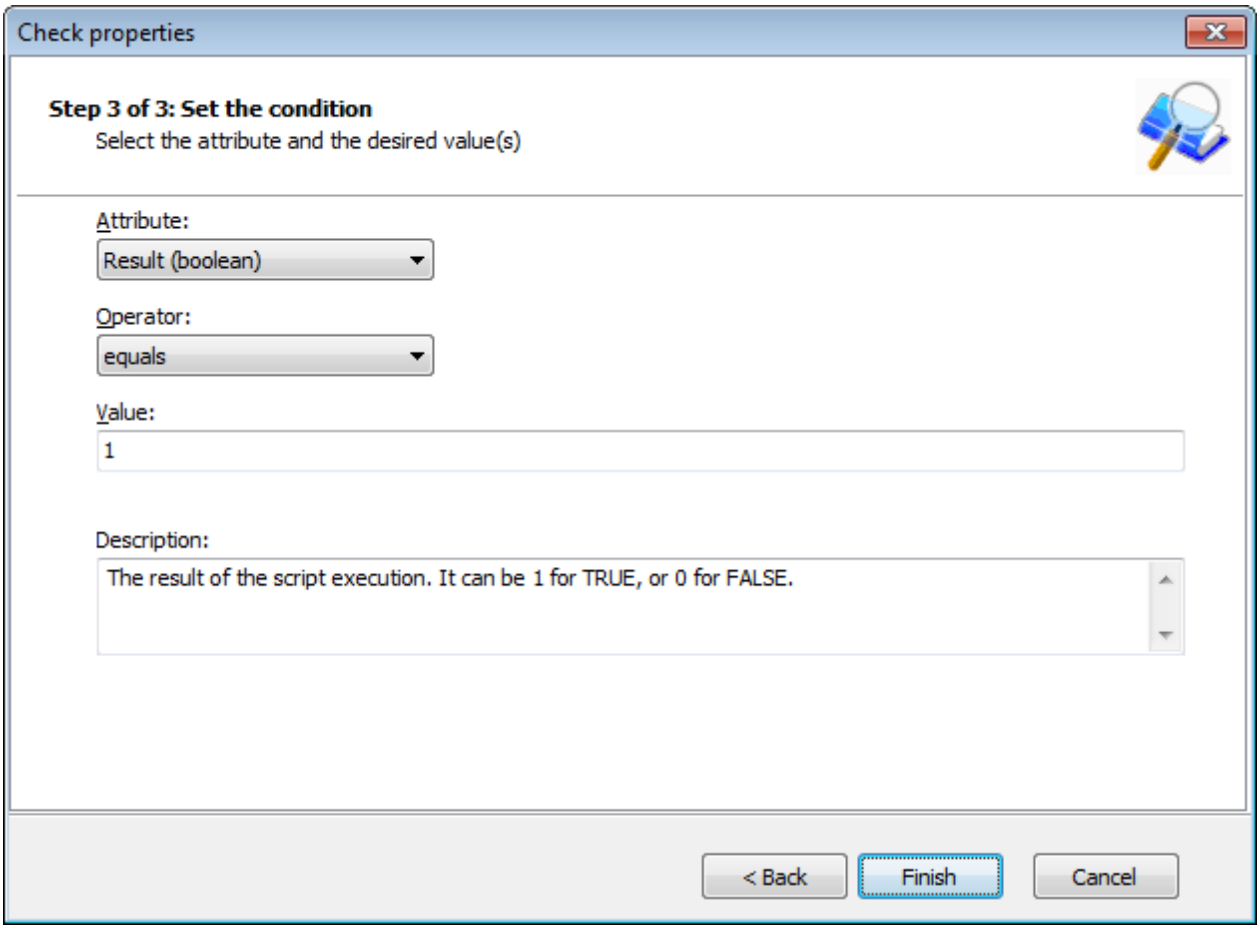
Screenshot 165: Adding vulnerability checks - Select type of check

7. Select **Unix checks > SSH Script Test** node and click on Next button to continue setup.


Check properties
Step 2 of 3: Define the object to examine
Set the properties of the object that must be checked
Object properties:
Properties
Values
Script file
sans06macskype.sh
Arguments
How many of the matching objects must satisfy the condition for the check to return TRUE:
at least one
Description:
A value of "at least one" means that at least one matching object must satisfy the data requirements for the check to evaluate to true. This is useful when regular expressions are used to define the object. In such cases it is possible that more than one object matches the definition.
< Back
Next >
Cancel

Screenshot 166: Adding vulnerability checks - Select SSH file

8. Click **Choose file** and select the custom SSH Script file that will execute during this check. Click **Next** to proceed.



Screenshot 167: Adding vulnerability checks - Define conditions

9. Select the relative condition setup in the wizard to finalize script selection. Click Finish to exit wizard.

10. Click **OK** to save new vulnerability check.

Step 3: Test the vulnerability check/script used in the example

Scan your local host computer using the scanning profile where the new check was added.

1. Log on to a Linux target computer and create a file called ‘test.file’. This check will generate a vulnerability alert if a file called 'test.file' is found.

2. Launch a scan on the Linux target where you created the file.

3. Check you scan results.

15 Miscellaneous

This chapter contains information about configuring NetBIOS on your computers and how to uninstall GFI LanGuard.

Topics in this chapter:

15.1 Configuring NetBIOS 243

15.2 Uninstalling GFI LanGuard 244

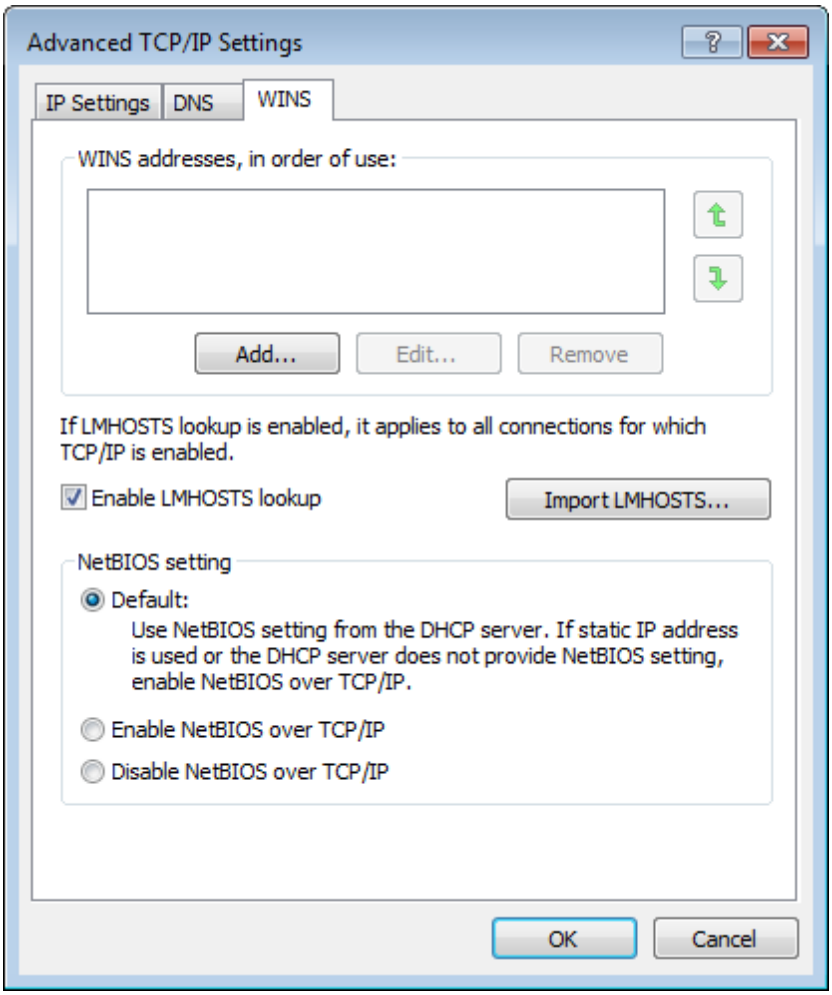
15.1 Configuring NetBIOS

To check if your scan targets are using NetBIOS:

1. Navigate to **Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings**.

> **Note**
>
> In Windows® XP, click **Control Panel > Network Connections**.

2. Right-click on **Local Area Connection** and select **Properties**.
3. Click **Internet Protocol (TCP/IP)** and select **Properties**.
4. Click **Advanced > WINS**.


Advanced TCP/IP Settings
IP Settings
DNS
WINS
WINS addresses, in order of use:
Add...
Edit...
Remove
If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.
Enable LMHOSTS lookup
Import LMHOSTS...
NetBIOS setting
Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.
Enable NetBIOS over TCP/IP
Disable NetBIOS over TCP/IP
OK
Cancel

Screenshot 168: Local Areas Connection properties: WINS tab

5. From the **NetBIOS setting** area, ensure that **Default** or **Enable NetBIOS over TCP/IP** are selected.
6. Click **OK** and exit the **Local Area Properties** dialog(s).

> **Note**
>
> If static IP is being used or the DHCP server does not provide NetBIOS setting, select the Enable NetBIOS over TCP/IP option.

15.2 Uninstalling GFI LanGuard

To uninstall GFI LanGuard:

1. Click **Start > Control Panel > Add or Remove Programs**.
2. Select GFI LanGuard from the list, and click **Remove**.
3. In the uninstall wizard, click **Next**.
4. Select the configuration data files to remove during un-installation and click **Next**.
5. On completion, click **Finish**.

16 Troubleshooting and support

This chapter explains how to resolve issues encountered while using GFI LanGuard. These issues can be resolved using the contents of this **Administrator Guide**. If any issues remain unresolved after reviewing the manual, check if your problem is listed below.

Refer to the following sections for information about resolving common issues and contacting our support team.

Topics in this chapter:

16.1 Resolving common issues 245

16.2 Using the Troubleshooter Wizard 247

16.3 GFI SkyNet 249

16.4 Web Forum 249

16.5 Requesting technical support 249

16.1 Resolving common issues

The table below provides you with solutions to the most common problems you may encounter when using GFI LanGuard:

Table 90: GFI LanGuard common Issues

Issue Encountered	Solution/Description
Failed to connect to database error is encountered when trying to configure the database backend.	**Description** This issue may occur when the following two conditions are met: 1. GFI LanGuard is installed on Windows 2000 SP4 with MDAC 2.5 SP 3 2. The database backend is SQL Server® having the database instance name different from the SQL Server® machine name. **Solution** Install **Microsoft® Data Access Components** (MDAC 2.6 or later) on GFI LanGuard machine and try again. MDAC can be downloaded from: http://go.gfi.com/?pageid=download_mdac
The database structure is incorrect. Do you want to delete and recreate the database? Warning is encountered when trying to configure the database back-end.	**Description** This issue occurs when the database structure is corrupted. Or The database returns a timeout because the connection cannot be established. **Solution** When this message is encountered: Check that all SQL credentials are correct and there are no connectivity problems between the GFI LanGuard machine and the SQL server. It is important to note that when OK is clicked all saved scans are lost.

Issue Encountered	Solution/Description
When trying to access the Change database tab while configuring an SQL database, a Failed to connect to database error is encountered	**Description** This issue may occur when the following two conditions are met: » GFI LanGuard is installed on Windows 2000 SP4 with MDAC 2.5 SP 3. » The database backend is SQL Server® having the database instance name different from the SQL Server® machine name. **Solution** Install Microsoft® Data Access Components (MDAC 2.6 or later) on the GFI LanGuard machine and try again. **Note** MDAC can be downloaded from: http://go.gfi.com/?pageid=download_mdac
Incomplete results and errors when scanning remote machines	**Description** Errors similar to the following may be encountered: » Failed to open test key to remote registry » The scan will not continue » Access Denied » Could not connect to remote SMB server. These errors may be encountered because: » The remote machine has an account similar to the one used by GFI LanGuard to log in as an administrator. » The user account used by GFI LanGuard does not have administrative privileges. **Solution** To solve this issue do one of the following: » Log on the GFI LanGuard machine and configure GFI LanGuard to use an alternate domain administrator account. » Delete the local user account on the remote machine. » Launch GFI LanGuard executable with 'Run As' using a Domain Administrator account. **Note** For more information, refer to http://go.gfi.com/?pageid=LAN_ProbScanningRM
GFI LanGuard program updates not working	**Description** Updates will not work if GFI LanGuard machine does not have a direct connection to the Internet. **Solution** To solve this issue do one of the following: » Configure GFI LanGuard machine to have direct Internet access. » Install another instance of GFI LanGuard on a machine with Internet access and configure GFI LanGuard to check for updates from the new installation. **Note** For more information refer to http://go.gfi.com/?pageid=LAN_CheckAltUpdates

Issue Encountered	Solution/Description
Firewall installed on GFI LanGuard is blocking connection with target computers	**Description** Scanning might slow down or be blocked if a firewall is installed on GFI LanGuard machine. **Solution** Configure the firewall to allow the following components in outbound connections: » <..\Program Files\GFI\LanGuard>*.exe » <..\Program Files\GFI\LanGuard Agent>*.exe **Note** For more information, refer to http://go.gfi.com/?pageid=LAN_SetBestPerformance
GFI LanGuard is failing to retrieve workgroup computers when using Enumerate Computers	**Description** GFI LanGuard uses the Windows mechanism to retrieve the machines within a workgroup. In this mechanism a Master Browser computer will create and store a list of all computers. In some cases, the Master Browser role can fail resulting in GFI LanGuard not retrieving computers information. **Note** To solve this issue, refer to http://go.gfi.com/?pageid=LAN_CannotEnumerate
GFI LanGuard found open ports that another port scanner found closed	**Description** GFI LanGuard uses a different approach than other port scanners to detect open ports. **Solution** To view the status of a port and determine if the port is closed or opened: 1. Click **Start > Programs > Accessories > Command Prompt**. 2. Key in `netstat -an`, and press **Enter**. 3. The generated list displays all computer active connections.

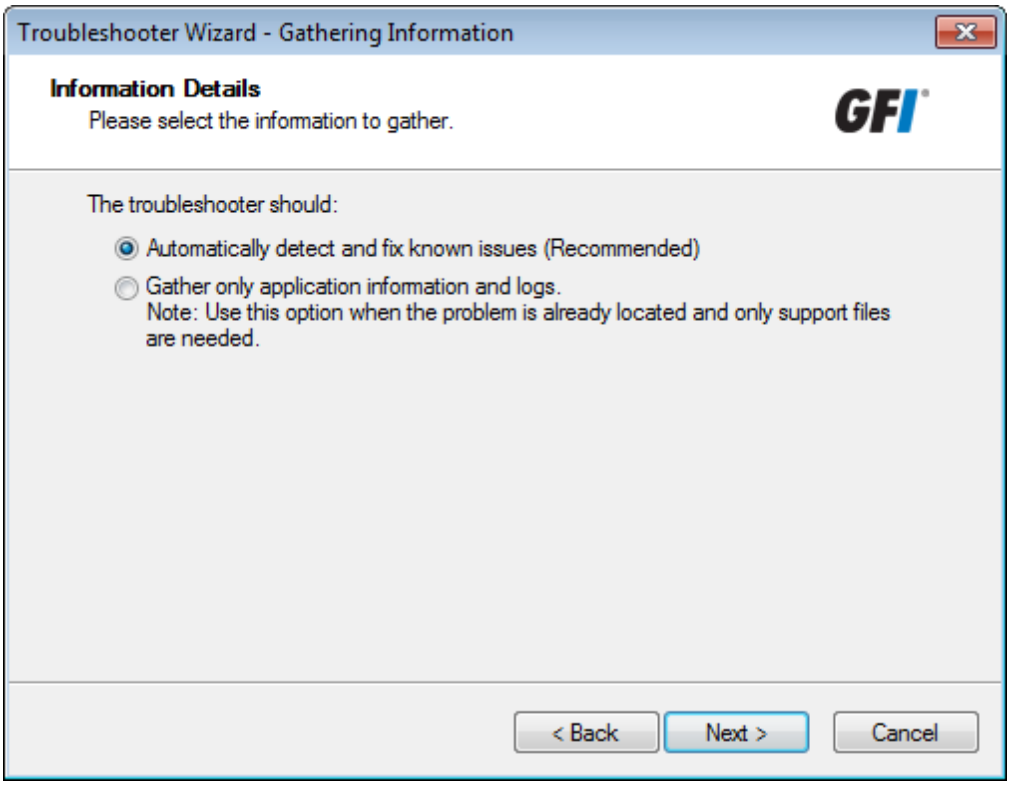
16.2 Using the Troubleshooter Wizard

The GFI LanGuard troubleshooter wizard is a tool designed to assist you when encountering technical issues related to GFI LanGuard. Through this wizard, you are able to automatically detect and fix common issues as well as gather information and logs to send to our technical support team.

To use the Troubleshooter Wizard:

1. Launch the troubleshooting wizard from the **Start > Programs > GFI LanGuard 2012 > GFI LanGuard 2012 Troubleshooter**.

2. Click **Next** in the introduction page.


Troubleshooter Wizard - Gathering Information
Information Details
Please select the information to gather.
GFI
The troubleshooter should:
Automatically detect and fix known issues (Recommended)
Gather only application information and logs.
Note: Use this option when the problem is already located and only support files are needed.
< Back
Next >
Cancel

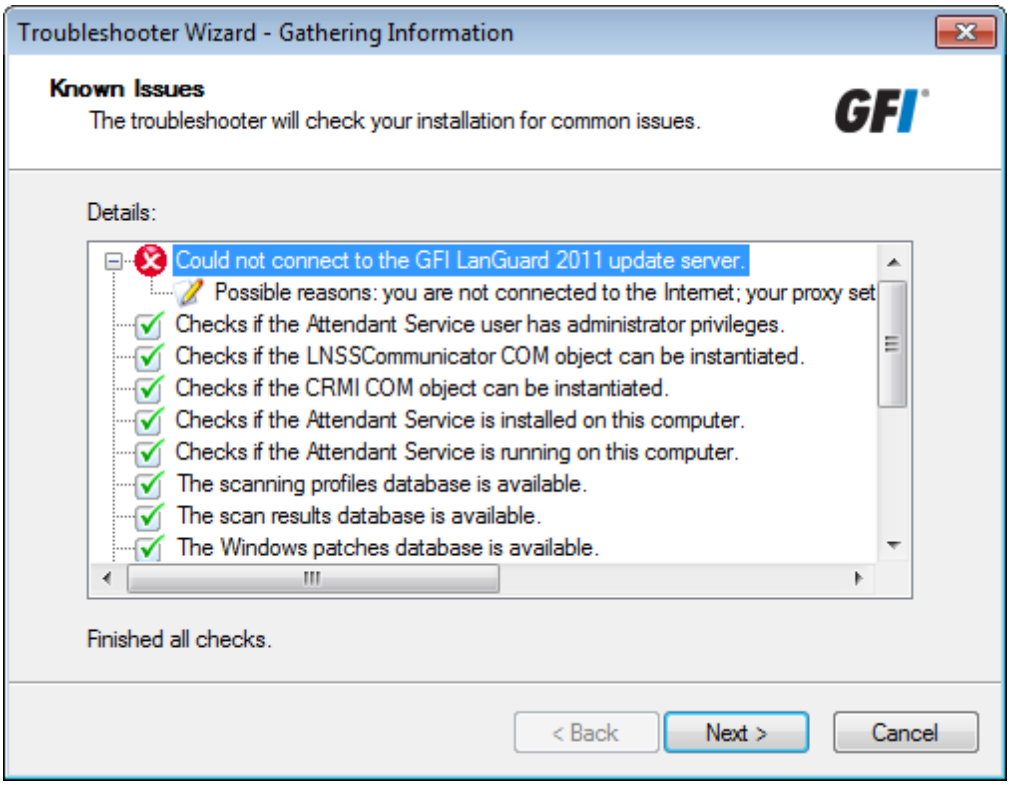
Screenshot 169: Troubleshooter wizard - Information details

3. In the Information details page select one of the following options described below:

Table 91: Information gathering options

Option	Description
Automatically detect and fix known issues	(Recommended) Configure GFI LanGuard to automatically detect and fix issues.
Gather only application information and logs	Gather logs to send to GFI support.

4. Click **Next** to continue.


Troubleshooter Wizard - Gathering Information
Known Issues
The troubleshooter will check your installation for common issues.
GFI
Details:
Could not connect to the GFI LanGuard 2011 update server.
Possible reasons: you are not connected to the Internet; your proxy set
Checks if the Attendant Service user has administrator privileges.
Checks if the LNSSCommunicator COM object can be instantiated.
Checks if the CRMI COM object can be instantiated.
Checks if the Attendant Service is installed on this computer.
Checks if the Attendant Service is running on this computer.
The scanning profiles database is available.
The scan results database is available.
The Windows patches database is available.
Finished all checks.
< Back
Next >
Cancel

Screenshot 170: Troubleshooter wizard - Gathering information about known issues

5. The troubleshooter wizard will retrieve all the information required to solve common issues. Click **Next** to continue.

6. The troubleshooter will fix any known issues that it encounters. Select **Yes** if your problem was fixed or **No** if your problem is not solved to search the GFI Knowledge base for information.

16.3 GFI SkyNet

GFI maintains a comprehensive knowledge base repository, which includes answers to the most common problems. GFI SkyNet always has the most up-to-date listing of technical support questions and patches. In case that the information in this guide does not solve your problems, next refer to GFI SkyNet by visiting http://kb.gfi.com/.

16.4 Web Forum

User to user technical support is available via the GFI web forum. Access the web forum by visiting http://forums.gfi.com

16.5 Requesting technical support

If none of the resources listed above enable you to solve your issues, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online**: Fill out the support request form and follow the instructions on this page closely to submit your support request on: http://support.gfi.com/supportrequestform.asp
- **Phone**: To obtain the correct technical support phone number for your region visit: http://www.gfi.com/company/contact.htm

Note

Before contacting Technical Support, have your Customer ID available. Your Customer ID is the online account number that is assigned to you when first registering your license keys in the GFI Customer Area at: http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

Documentation

If this manual does not satisfy your expectations, or if you think that this documentation can be improved in any way, let us know via email on documentation@gfi.com.

17 Appendix 1 - Data Processed

When auditing networks, GFI LanGuard enumerates and processes the following information. This information is collected from scan targets using the ports and protocols described in the following sections.

Topics in this chapter:

17.1 System Patching Status 251

17.2 Ports 252

17.3 Hardware 252

17.4 Software 254

17.5 System Information 256

17.1 System Patching Status

Data	Description	Ports	Protocol
Missing Service Packs and Update Rollups	Discovers missing Microsoft® and non-Microsoft® service packs.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » Windows update agent.
Missing Security Updates	Discovers missing Microsoft® and non-Microsoft® patches.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » Windows update agent.
Missing Non-Security Updates	Lists installed Microsoft® and non-Microsoft® service packs.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » Windows update agent.

Data	Description	Ports	Protocol
Installed Service Packs and Update Rollups	Lists installed Microsoft® and non-Microsoft® patches.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » Windows update agent.
Installed Security Updates	Lists installed Microsoft® and non-Microsoft® service packs.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » Windows update agent.
Installed Non-Security Updates	Lists installed Microsoft® and non-Microsoft® patches.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » Windows update agent.

17.2 Ports

Data	Description	Ports	Protocol
Open TCP ports	Checks for open TCP ports.	All enabled ports in the scan profile.	Windows sockets.
Open UDP ports	Checks for open UDP ports.	All enabled ports in the scan profile.	Windows sockets.

17.3 Hardware

Data	Description	Ports	Protocol
Network devices	Lists physical and virtual network adapters.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » WMI.

Data	Description	Ports	Protocol
Local drives	Lists drives discovered on scanned target(s). Local drives include: » Hard disks » CD/DVD drives » Floppy drives	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » WMI.
Processors	Lists processors discovered during a scan.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » WMI.
Motherboards	Lists motherboards discovered during a scan.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » WMI.
Memory details	Returns memory information of scanned target(s), including: » Total physical memory » Free physical memory » Total virtual memory » Free virtual memory.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » WMI.
Storage details	Lists every storage device discovered during a scan. Storage devices include: » Hard disks » Virtual hard disks » Removable disks » Floppy drives » CD/DVD drives.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » WMI.
Display adapters	Lists video cards discovered during a scan	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » WMI.

Data	Description	Ports	Protocol
USB Devices	Lists all the detected USB devices that are attached to the network/scan targets.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » WMI.
Other devices	Lists generic devices discovered during a scan, including: » System devices/drivers » Human Interface Devices (HID) » Mouse and keyboard » Communication ports (Serial and Parallel) » Floppy disk controllers » Hard disk controllers.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic.	» SMB » File and printer sharing » Remote registry » WMI.

17.4 Software

Data	Description	Ports	Protocol
General applications	Enumerates every application installed on the scan target(s).	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Antiphishing applications	Lists antiphishing applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Antispyware applications	Lists antispyware applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Antivirus applications	Lists antivirus applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry

Data	Description	Ports	Protocol
Backup applications	Lists backup applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Data Loss Prevention	Lists Data Loss Prevention applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Device Access Control	Lists Device Access Control applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Disk Encryption	Lists Disk Encryption applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Firewall applications	Lists firewall applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Health Agent	Lists system health monitoring applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Instant Messenger	Lists Instant Messenger applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Patch management applications	Lists patch management applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry

Data	Description	Ports	Protocol
Peer To Peer	Lists Peer to Peer (P2P) applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
URL Filtering	Lists web filtering applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Virtual Machine Software	Lists virtualization software detected on your network.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Virtual Private Network (VPN) Client applications	Lists VPN client applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Web Browser applications	Lists web browsers.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry

Note

For a full list of supported security applications including vendors and products, refer to http://go.gfi.com/?pageid=security_app_fullreport

17.5 System Information

Data	Description	Ports	Protocol
Shares	Lists all shares discovered during a scan. Shares information include: » Share name » Share remark » Share path » Share permissions.	» TCP 139 » TCP 445.	» SMB » File and printer sharing » Remote registry

Data	Description	Ports	Protocol
Password policy	Lists password policy configuration.	» TCP 139 » TCP 445.	» SMB » File and printer sharing » Remote registry.
Security audit policy	Security audit policy configuration.	» TCP 139 » TCP 445.	» SMB » File and printer sharing » Remote registry.
Registry	Lists selected information from the system registry. Amongst others, enumerated information includes: » Registry owner » Current build number » Current type » Current version » Vendor identifier » Software type.	» TCP 139 » TCP 445.	» SMB » File and printer sharing » Remote registry.
NetBIOS names	Lists NetBIOS names of the scanned target(s). This node includes: » Workstation service » Domain name » File server services » Browser service elections.	» TCP 139 » TCP 445.	» SMB » File and printer sharing » Remote registry.
Computer	Lists computer identifiers including: » MAC address » Time to live » Network role » OS Serial number » Language » Machine type (physical or virtual).	» TCP 139 » TCP 445.	» SMB » File and printer sharing » Remote registry.
Groups	Lists local or domain/workgroup groups.	» TCP 139 » TCP 445.	» SMB » File and printer sharing » Remote registry.
Users	Lists local or domain/workgroup users.	» TCP 139 » TCP 445.	» SMB » File and printer sharing » Remote registry.

Data	Description	Ports	Protocol
Logged on users	Lists locally and remotely logged on users.	» TCP 139 » TCP 445.	» SMB » File and printer sharing » Remote registry.
Sessions	Lists the active sessions at the time of the scan.	» TCP 139 » TCP 445.	» SMB » File and printer sharing » Remote registry.
Services	Lists every service discovered during a scan.	» TCP 139 » TCP 445.	» SMB » File and printer sharing » Remote registry.
Processes	Lists every active process discovered during a scan.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry.
Remote TOD (time of day)	Lists the current time and uptime of the scanned target(s).	» TCP 139 » TCP 445.	» SMB » File and printer sharing » Remote registry.

18 Appendix 2 - Certifications

GFI LanGuard is OVAL and CVE certified. The following sections describe each certification and explain how they are used in GFI LanGuard.

Topics in this chapter:

18.1 Open Vulnerability and Assessment Language (OVAL) 259

18.2 Common Vulnerabilities and Exposures (CVE) 260

18.1 Open Vulnerability and Assessment Language (OVAL)

Open Vulnerability and Assessment Language (OVAL™) is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the OVAL community. The language standardizes the three main steps of the assessment process:

- Representing configuration information of systems for testing
- Analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.)
- Reporting the results of this assessment.
- The repositories are collections of publicly available and open content that utilize the language.

The OVAL community has developed three XML schemas to serve as the framework and vocabulary of the OVAL Language. These schemas correspond to the three steps of the assessment process:

- An OVAL System Characteristics schema for representing system information
- An OVAL Definition schema for expressing a specific machine state
- An OVAL Results schema for reporting the results of an assessment

Content written in OVAL Language is located in one of the many repositories found within the community. One such repository, known as the OVAL Repository, is hosted by MITRE Corporation. It is the central meeting place for the OVAL Community to discuss, analyze, store, and disseminate OVAL Definitions. Each definition in the OVAL Repository determines whether a specified software vulnerability, configuration issue, program, or patch is present on a system.

The information security community contributes to the development of OVAL by participating in the creation of the OVAL Language on the OVAL Developers Forum and by writing definitions for the OVAL Repository through the OVAL Community Forum. An OVAL Board consisting of representatives from a broad spectrum of industry, academia, and government organizations from around the world oversees and approves the OVAL Language and monitors the posting of the definitions hosted on the OVAL Web site. This means that the OVAL, which is funded by US-CERT at the U.S. Department of Homeland Security for the benefit of the community, reflects the insights and combined expertise of the broadest possible collection of security and system administration professionals worldwide.

18.1.1 GFI LanGuardOVAL Support

GFI LanGuard supports all checks defined in the XML file issued by OVAL, with the exception of HP-UX checks.

GFI LanGuard does not support HP-UX based machines and therefore it is beyond the scope of this product to include these checks within its check definition database.

18.1.2 About OVAL Compatibility

OVAL Compatibility is a program established to develop consistency within the security community regarding the use and implementation of OVAL. The main goal of the compatibility program is to create a set of guidelines that will help enforce a standard implementation. An offshoot of this is that users are able to distinguish between, and have confidence in, compatible products knowing that the implementation of OVAL coincides with the standard set forth.

For a product or service to gain official OVAL Compatibility, it must adhere to the **Requirements and Recommendations for OVAL Compatibility** and complete the formal OVAL Compatibility Process.

OVAL Compatibility means that GFI LanGuard incorporates OVAL in a pre-defined, standard way and uses OVAL for communicating details of vulnerabilities, patches, security configuration settings, and other machine states.

18.1.3 Submitting OVAL listing error reports

Any issues with the GFI LanGuard or the listing of the OVAL checks included with GFI LanGuard should be reported to GFI through its official support lines.

GFI Software Ltd will endeavor to look into any issues reported and if any inconsistency or error is ascertained, it will issue updates to fix such issues. Vulnerability check updates are usually released on monthly basis.

18.2 Common Vulnerabilities and Exposures (CVE)

CVE (Common Vulnerabilities and Exposures) is a list of standardized names for vulnerabilities and other information security exposures. Its aim is to standardize the names for all publicly known vulnerabilities and security exposures.

CVE is a dictionary which aim is to facilitate data distribution across separate vulnerability databases and security tools. CVE makes searching for information in other databases easier and should not be considered as a vulnerability database by itself.

CVE is a maintained through a community-wide collaborative effort known as the CVE Editorial Board. The Editorial Board includes representatives from numerous security-related organizations such as security tool vendors, academic institutions, and governments as well as other prominent security experts. The MITRE Corporation maintains CVE and moderates editorial board discussions.

18.2.1 About CVE Compatibility

"CVE-compatible" means that a tool, Web site, database, or service uses CVE names in a way that allows it to cross-link with other repositories that use CVE names. CVE-compatible products and services must meet the four requirements:

Table 92: CVE Compatibility

Compatibility	Description
CVE Searchable	A user must be able to search for vulnerabilities and related information using the CVE name.
CVE Output	Information provided must include the related CVE name(s).
Mapping	The repository owner must provide a mapping relative to a specific version of CVE, and must make a good faith effort to ensure accuracy of that mapping.
Documentation	The organization's standard documentation must include a description of CVE, CVE compatibility, and the details of how its customers can use the CVE-related functionality of its product or service.

Note

For an in-depth understanding of CVE compatibility refer to the complete list of CVE requirements available at http://go.gfi.com/?pageid=LAN_CVE_Requirements

18.2.2 About CVE and CAN

CVE names (also called "CVE numbers," "CVE-IDs," and "CVEs") are unique, common identifiers for publicly known information security vulnerabilities. CVE names have "entry" or "candidate" status. Entry status indicates that the CVE name has been accepted to the CVE List while candidate status (also called "candidates," "candidate numbers," or "CANs") indicates that the name is under review for inclusion in the list.

Each CVE name includes the following:

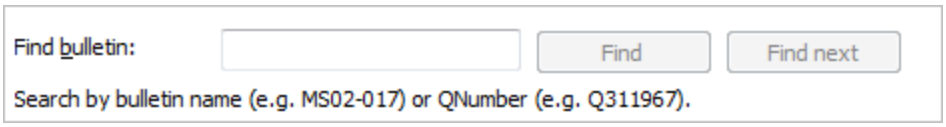
- CVE identifier number (i.e. "CVE-1999-0067").
- Indication of "entry" or "candidate" status.
- Brief description of the security vulnerability or exposure.
- Any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID).

Note

For an in-depth understanding of CVE names and CANs, refer to: http://go.gfi.com/?pageid=cvecert

18.2.3 Searching for CVE Entries

CVE entries can be searched from the Scanning profiles node within the Configuration tab.



Screenshot 171: Searching for CVE information

To search for a particular CVE bulletin:

1. Specify the bulletin name (for example, CVE-2005-2126) in the search tool entry box included at the bottom of the right pane.

2. Click on **Find** to start searching for your entry.

18.2.4 Obtaining CVE Names

CVE entry names can be obtained through the GFI LanGuard user interface from within the Scanning profiles node within the Configuration tab. By default, the CVE ID is displayed for all the vulnerabilities that have a CVE ID.

18.2.5 Importing and Exporting CVE Data

CVE data can be exported through the impex command line tool. For more information, refer to Using impex.exe (page 226).

19 Glossary

A

Access™

A Microsoft® desktop relational database management system included in the Microsoft® Office package. Access™ is normally used for small databases.

Active Directory™ (AD)

A technology that provides a variety of network services, including LDAP-like directory services.

Anti-spyware

A software countermeasure that detects spyware installed on a computer without the user's knowledge.

Antivirus

A software countermeasure that detects malware installed on a computer without the user's knowledge.

Apache web server

An open source HTTP server project developed and maintained by the Apache software foundation.

Applications auto-uninstall

An action that enables the auto-uninstall of applications that support silent uninstall from GFI LanGuard.

Auto-download

A GFI LanGuard technology that automatically downloads missing patches and service packs in all 38 languages.

Auto-patch management

A GFI LanGuard technology that automatically downloads missing Microsoft® updates and deploys them over the network.

Auto-remediation

A GFI LanGuard technology that automatically downloads and deploy missing patches. If an application is blacklisted in GFI LanGuard, auto-remediation will uninstall the application from the target computer during scheduled operations.

B

Backdoor program

An alternative method used to access a computer or computer data over a network.

Batch-files

A text files containing a collection of instructions to be carried out by an operating system or an application.

Blacklist

A list of USBs or Network devices names that are considered as dangerous. When a USB\Network device name contains a blacklisted entry while scanning a network, GFI LanGuard will report the device as a security threat (High security vulnerability).

Bluetooth

An open wireless communication and interfacing protocol that enables exchange of data between devices.

Bulletin Information

Contains a collection of information about a patch or a Microsoft® update. Used in GFI LanGuard to provide more information on an installed patch or update. Information includes; Bulletin id, title, description, URL and file size.

C

Common Gateway Interface (CGI)

A communication script used by web servers to transfer data to a client internet browser.

Common Vulnerabilities and Exposures (CVE)

A list of standardized names for vulnerabilities and other information security exposures. The aim of CVE is to standardize the names for all publicly known vulnerabilities and security exposures.

D

Dashboard

A graphical representation that indicates the status of various operations that might be currently active, or that are scheduled.

Demilitarized Zone (DMZ)

A section of a network that is not part of the internal network and is not directly part of the Internet. Its purpose typically is to act as a gateway between internal networks and the internet.

deploycmd.exe

A GFI LanGuard command line tool, used to deploy Microsoft® patches and third party software on target computers.

DMZ

A section of a network that is not part of the internal network and is not directly part of the Internet. Its purpose typically is to act as a gateway between internal networks and the internet.

DNS

A database used by TCP/IP networks that enables the translation of hostnames into IP numbers and to provide other domain related information.

DNS Lookup tool

A utility that converts domain names into the corresponding IP address and retrieves particular information from the target domain

Domain Name System

A database used by TCP/IP networks that enables the translation of hostnames into IP numbers and to provide other domain related information.

E

Enumerate computers tool

A utility that identifies domains and workgroups on a network.

Enumerate users tools

A tools which enables you to retrieve users and user information from your domain/workgroup.

Extensible Markup Language (XML)

An open text standard used to define data formats. GFI LanGuard uses this standard to import or export scanned saved results and configuration.

F

File Transfer Protocol

A protocol used to transfer files between network computers.

FTP

A protocol used to transfer files between network computers.

G

GFI EndPointSecurity

A security solution developed by GFI that helps organizations to maintain data integrity by preventing unauthorized access and transfers from removable devices.

GPO

An Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.

Group Policy Object (GPO)

An Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.

I

ICMP pings

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is used by the operating systems of networked computers to send error

messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.

impex.exe

A Command line tool, used to Import and Export profiles and vulnerabilities from GFI LanGuard.

Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.

Internet Information Services (IIS)

A set of Internet-based services created by Microsoft® Corporation for internet servers.

L

Linux

An open source operating system that is part of the Unix operating system family.

lnsscmd.exe

A GFI LanGuard command line tool that allows running vulnerability checks against network targets.

Local Host

In networking, the local host is the computer you are currently using. One can reference to the local host by using the reserved IP address 127.0.0.1. In this manual the Local host is the machine where GFI LanGuard is installed.

M

Mail server

The server that manages and stores client emails.

Malware

Composed from malicious and software, malware is a general term used for all software developed to harm and damage a computer system. Viruses, worms and Trojans are all type of malware.

Microsoft® Access™ database

A Microsoft® desktop relational database management system included in the Microsoft® Office package. Microsoft® Access™ is normally used for small databases.

Microsoft® IIS

A set of Internet-based services created by Microsoft® Corporation for internet servers.

Microsoft® Windows service packs

A collection of updates and fixes provided by Microsoft® to improve an application or an operating system.

Microsoft® WSUS

An acronym for Microsoft® Windows Server Update Services. This service enables administrators to manage the distribution of Microsoft® updates to network computers.

N

NETBIOS

An acronym for Network Basic Input/output. This system provides services to allow applications on different computers within a network to communicate with each other.

Netscape

A web browser originally developed by Netscape Communications Corporation.

O

Open Vulnerability and Assessment Language (OVAL)

A standard that promotes open and publicly available security content, and standardizes the transfer of this information across the entire spectrum of security tools and services.

OVAL

A standard that promotes open and publicly available security content, and standardizes the transfer of this information across the entire spectrum of security tools and services.

P

Patch agent

A background service that handles the deployment of patches, service packs and software updates on target computers.

Python scripting

A high-level computer programming scripting language.

R

Remote Desktop Protocol

A protocol developed by Microsoft® to enable clients to connect with the user interface of a remote computer.

S

SANS

An acronym for System Administration, Networking and Security research organization. An institute that shares solutions regarding system and security alerts.

Scan profiles

A collection of vulnerability checks that determine what vulnerabilities are identified and which information will be retrieved from scanned targets.

Script Debugger

A GFI LanGuard module that allows you to write and debug custom scripts using a VBScript-compatible language.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol is a technology used to monitor network devices such as, routers, hubs and switches.

SNMP

Acronym for Simple Network Management Protocol, a technology used to monitor network devices such as, routers, hubs and switches.

SNMP Auditing tool

A tool that reports weak SNMP community strings by performing a dictionary attack using the values stored in its default dictionary.

SNMP Walk tool

A tool used to probe your network nodes and retrieve SNMP information.

Spyware

A form of malware intended to collect information from a computer without notifying the user.

SQL Server Audit tool

A tool used to test the password vulnerability of the -sa- account (i.e. root administrator), and any other SQL user accounts configured on the SQL Server.

SQL Server®

A Microsoft® relational database management system. Microsoft® included extra functionality to the SQL Server® (transaction control, exception handling and security) so that Microsoft® SQL server can support large organizations.

SSH Module

A module used to determine the result of vulnerability checks through the console (text) data produced by an executed script. This means that you can create custom Linux/UNIX vulnerability checks using any scripting method that is supported by the target-s Linux/UNIX OS and which outputs results to the console in text.

T

TCP ports

Acronym for Transmitting Control Protocol. This protocol is developed to allow applications to transmit and receive data over the internet using the well-known computer ports.

Terminal Services

A service that allows connecting to a target computer and managing its installed applications and stored data.

Traceroute tool

A tool used to identify the path that GFI LanGuard followed to reach a target computer.

Trojans

A form of malware that contains a hidden application that will harm a computer.

U

UDP ports

An acronym for User Datagram Protocol, these used to transfer UDP data between devices. In this protocol received packets are not acknowledged.

Uniform Resource Locator (URL)

The Uniform Resource Locator is the address of a web page on the world wide web.

Universal Serial Bus (USB)

A Serial bus standard widely used to connect devices to a host computer.

URL

The Uniform Resource Locator is the address of a web page on the world wide web.

V

VBScript

A Visual Basic Scripting language is a high-level programming language developed by Microsoft®.

Virus

A form of malware that infects a computer. The aim of a virus is to harm a computer by corrupting files and applications. A virus is a self-replicating program and can copy itself all over the computer system.

W

Web server

A server that provides web pages to client browsers using the HTTP protocol.

White-list

A list of USBs or Network devices names that are not considered as dangerous. When a USB/Network device name contains a white-listed entry while scanning a network, GFI LanGuard will ignore the device and consider it as a safe source.

Whois tool

A tool that enables you to look up information on a particular domain or IP address.

Wi-Fi/Wireless LAN

A technology used commonly in local area networks. Network nodes use data transmitted over radio waves instead of cables to communicate with each other.

X

XML

An open text standard used to define data formats. GFI LanGuard uses this standard to import or export scanned saved results and configuration.

20 Index

A

Activity 70, 81, 93, 151, 157-159, 170, 211, 221

Advanced 24, 45, 51, 53-54, 84, 117, 129, 132, 134, 141, 143, 145, 147, 149, 171, 175, 178, 198, 206, 243

Agent 23, 38, 47, 61, 80, 82, 93, 95, 101, 125, 136, 138, 153, 160, 209, 247, 251, 255

Agent-based 19

Agent-less 17, 19, 25, 64, 101

Alerting Options 77, 169, 177, 223

Antiphishing 96, 254

Antispyware 96, 254

Applications scanning options 202

Attendant service 18, 34, 74

Attributes 46, 50, 62, 86, 88, 96, 161

Audit 61, 69-70, 83, 93, 95, 97, 99-102, 117, 159, 203, 220, 222

Audit schedule 45

Auto-deployment 116-117, 155

auto-download 70, 117, 155

Auto-remediation 38, 75, 116, 125, 132, 136

Auto-Update 184

B

Backup 96, 113, 255

Baseline Comparison 162

Bulletin Info 140

C

Certifications 259

CGI 199

Check 31-32, 41, 62, 109, 119, 155, 228, 243, 245

Client 17, 19, 51, 53, 112, 131, 256

Command Line Tools 18, 223

Common Vulnerabilities and Exposures 260

Complete/Combination scans 64, 210

Compliance 38, 42, 159

Components 17, 23, 31, 34, 245

Computer 17, 34, 37, 47, 52, 82, 84, 92, 105, 124-125, 130, 132, 136, 138-139, 141, 143, 145, 155, 192, 213, 215, 220-221, 223, 233, 257

Computer Security Overview 160

Computer Summary 161

Computer Tree 47, 54, 61, 67, 80, 84, 88, 106, 125, 140, 142, 144, 156, 165, 167, 174

Conditions 163, 189, 230, 234, 239, 245

Custom 18, 39, 41, 44, 46, 53, 64, 67, 127, 139, 144-145, 167, 188, 211, 218, 228, 233, 237

Custom target properties 67

CVE 260

D

Daily Digest 173, 178

Dashboard 39-40, 45, 47, 58, 69, 80, 82-84, 88, 90-92, 97-103, 106, 225

database retention options 183

Deploy custom software 138

Deploy Software Updates 132, 138-139

deploycmd.exe 223

Device scanning options 202

DHCP 244

Display adapters 111, 253

DNS 52, 108, 213

DNS Lookup 212

Drivers 113, 254

E

Enumerate Computers 40, 217, 247

Enumerate Users 219

Export 32, 35, 46, 145, 169

F

File and printer sharing 251-252, 254, 256

Find 84, 118, 146, 148, 201, 261

Firewall applications 112, 255

Floppy disk controllers 254

Footer 173

Full Audit 161

G

General applications 254

Groups 87, 89, 96, 106, 156, 162, 257

H

Hardware 16, 23, 40-41, 66, 87, 91, 96, 102, 111, 161, 206, 252

Hardware Audit 66, 161

Header 172

Human Interface Devices (HID) 254

I

IIS 108

impex.exe 226

Import 30, 35, 44-45, 71, 145, 226

Install 18, 30, 35, 149, 169, 173

Installed Non-Security Updates 110, 142, 252

Installed Security Updates 110, 142, 163, 252

Installed Service Packs and Update Rollups 110, 142, 162, 252

Installing 17, 19, 38, 74, 116, 154, 184, 225

L

Last Auto-remediation 161

Last Scan Details 161

Last Scan Security Changes 161

Last Scan Summary 161

Level 83, 90, 92, 106, 160, 230, 234, 239

List scanned computers 178

lnsscmd.exe 223

Loading Results 113

Local drives 111, 253

Logged on users 113, 258

M

Malware 39, 94, 138-139, 147

Management Console 17, 21, 35, 223, 238

Memory details 111, 253

Messages 116, 127, 132

Missing Non-Security Updates 110, 139, 251

Missing Security Updates 109, 139, 160, 251

Missing Service Packs and Update Rollups 95, 109, 139, 251

Monitor 19, 58, 69, 78, 141, 143, 163, 170, 212

Motherboards 253

Mouse and keyboard 254

N

NetBIOS 26, 138, 210, 217, 243, 257

Network & Software Audit 42, 66, 104, 202

Network devices 66, 111, 204, 210, 252

Network Security History 162

Network Security Overview 160

Notifications 18, 178

O

Open Ports 161

Open Shares 161

Open TCP ports 96, 252

Open UDP ports 96, 252

Open Vulnerability and Assessment Language 259

OVAL 16, 192, 259, 261

P

Password 34, 44, 69, 112, 145, 147-148, 178, 185, 222-223, 237, 257

Patch management 255

Patching Status 160

PCI DSS 42, 162

Ports 23, 27, 65, 91, 93, 96, 100, 110, 203, 211, 247, 251-252, 254, 256

Processors 96, 111, 253

Product Updates 51, 63, 154, 158, 208

Profiles 65, 177, 189-190, 200, 203, 210, 261

Protocols 25

Proxy 38, 154, 184, 199

Python 233

R

Real-time 91

References 192, 230, 234

Registry 17, 25, 108, 162, 211, 227, 246, 257

Relay Agents 17, 19, 24, 53, 93

Remediation Center 90, 119, 132, 138, 144-145, 148, 150

Remediation History 162

Remediation Jobs 141, 143, 145, 147, 149, 155

Remediation Operations 17, 25, 54, 116, 155

Remote Desktop Connection 139, 149

Remote registry 251-252, 254, 256

S

Saved scan results 181

Scan Based – Full Audit 161

Scan History 162

Scanning Profile Editor 188-189, 200, 210, 229, 234, 239

Scanning Profiles 18, 27, 64, 70, 116-117, 123, 188-189, 200, 202, 210, 223, 229, 234, 239

Scheduled Scans 38, 70, 80, 93, 122, 153

Script Debugger 228

Security audit policy 69, 257

Security Scanning Options 209

Security Scans 18, 70, 83, 151, 159, 163

Security Updates 26, 38, 64, 95, 119, 144, 153, 160, 189, 199

Server 17-19, 23, 51, 53, 62, 65, 67, 169, 178, 184, 199, 211, 222-223, 245, 257

Sessions 18, 113, 223, 258

Shares 53, 66, 112, 127, 143, 162, 204, 211, 256

SMB 17, 26, 246, 251-252, 254, 256

SMTP 108, 178

SNMP 26, 66, 210, 220-221

SNMP Auditing 220

SNMP Walk 221

Software 23, 30, 38-42, 66, 80, 91, 94, 96, 101, 108, 116-117, 127, 138-139, 142, 144, 153-154, 175, 185, 199, 202, 218, 224, 254, 257, 259

Software Audit 41-42, 64, 114-115, 161

SQL 25, 114, 178, 222, 245

SQL Server Audit 222

SSH 25, 69, 74, 211, 237

Storage details 111, 253

System Information 40-41, 65, 91, 103, 112, 161, 202, 256, 259

System Patching Status 110, 251

T

TCP/UDP port scanning options 202

Traceroute 215

U

Unauthorized 16, 41, 76, 96, 108, 121, 137, 145, 161, 204

Unauthorized Applications 94, 116, 161, 207

Uninstall 17, 27, 45, 52, 76, 93, 116, 121, 137

Uninstall Applications 138-139, 145, 174

Uninstall Software Updates 138-139, 142

Upgrading 30

USB 204, 254

Users 87, 96, 108, 164, 219, 225, 228, 257, 260

Utilities 212, 215-217, 219-222

V

VBscript 228

VPN client applications 256

Vulnerabilities 39-42, 64-65, 88, 90-92, 95, 98, 106, 116, 128, 138, 147, 160, 184, 189, 201, 206, 226, 239, 260

Vulnerability Assessment 16, 27, 38, 64, 104, 114-115, 189, 200, 210, 228, 233

Vulnerability Level Rating 104

Vulnerability Management Strategy 38

Vulnerability Status 160

W

Wake-on-LAN 69, 75, 116, 130

Whois 216

WINS 244

WMI 25, 211, 252

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104 Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.com

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

GFI®